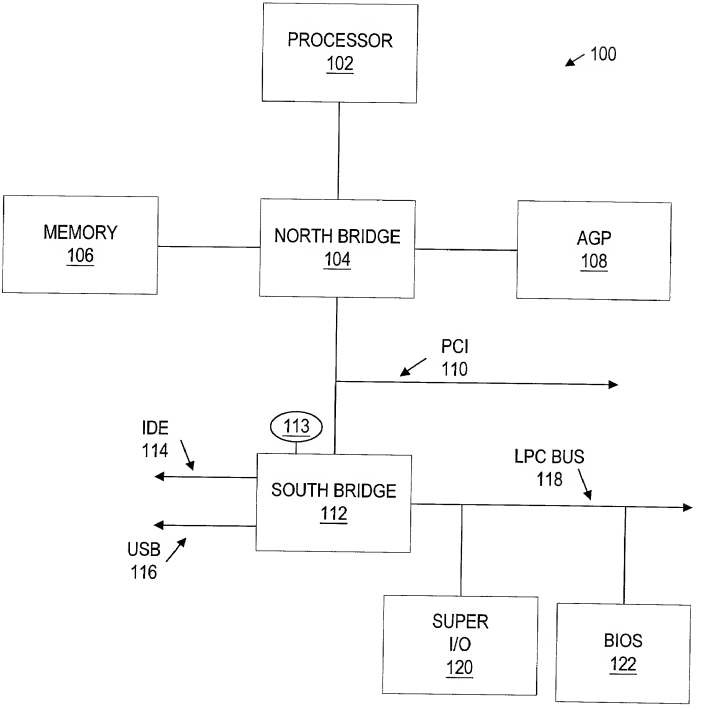

Fig. 1A
(Prior Art)

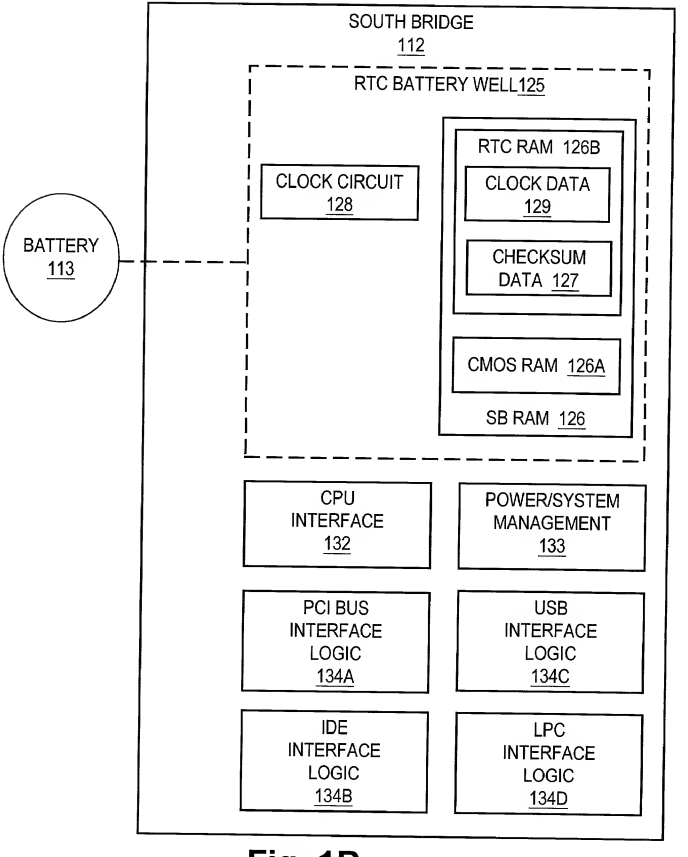

Fig. 1B
(Prior Art)

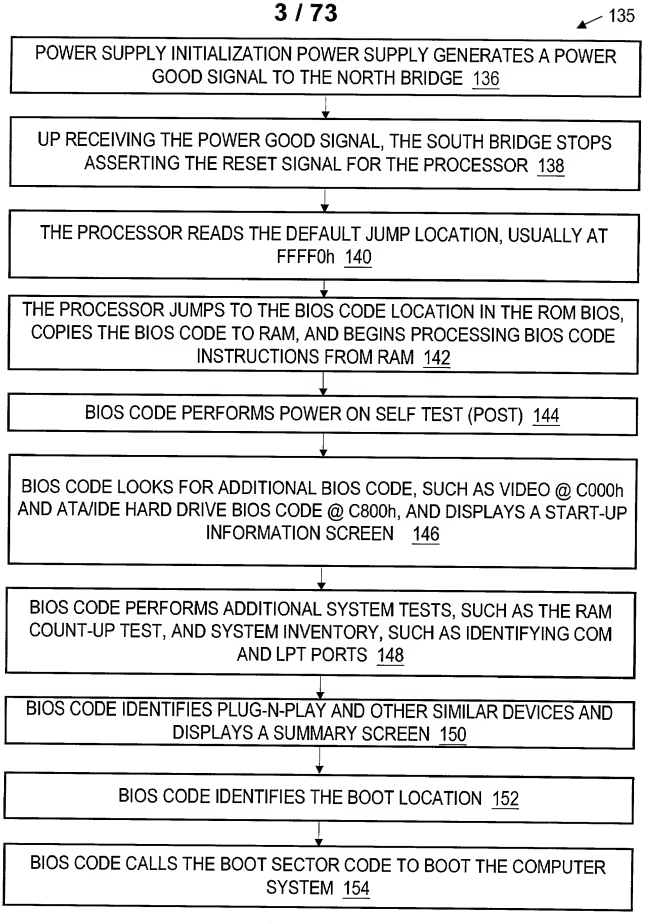

Fig. 2A
(Prior Art)

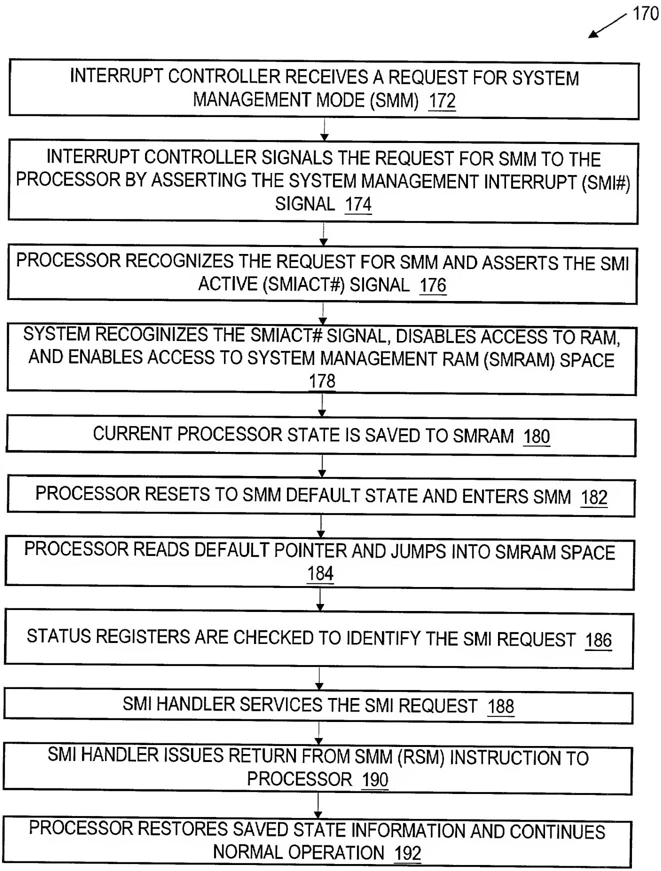

Fig. 2B
(Prior Art)

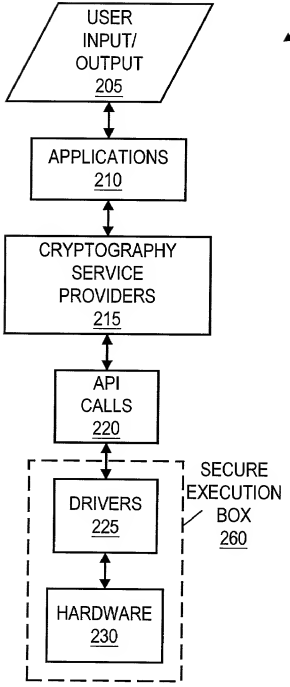

Fig. 3

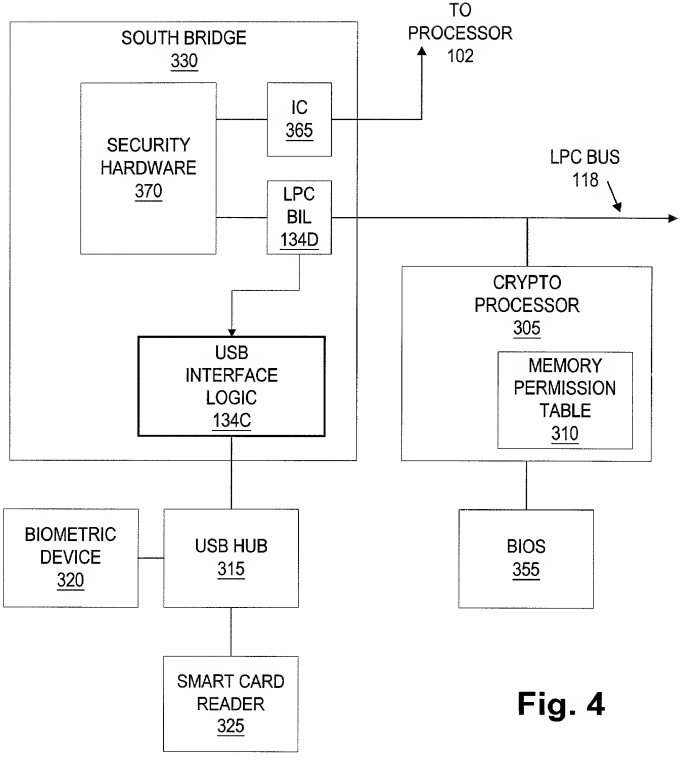

Fig. 4

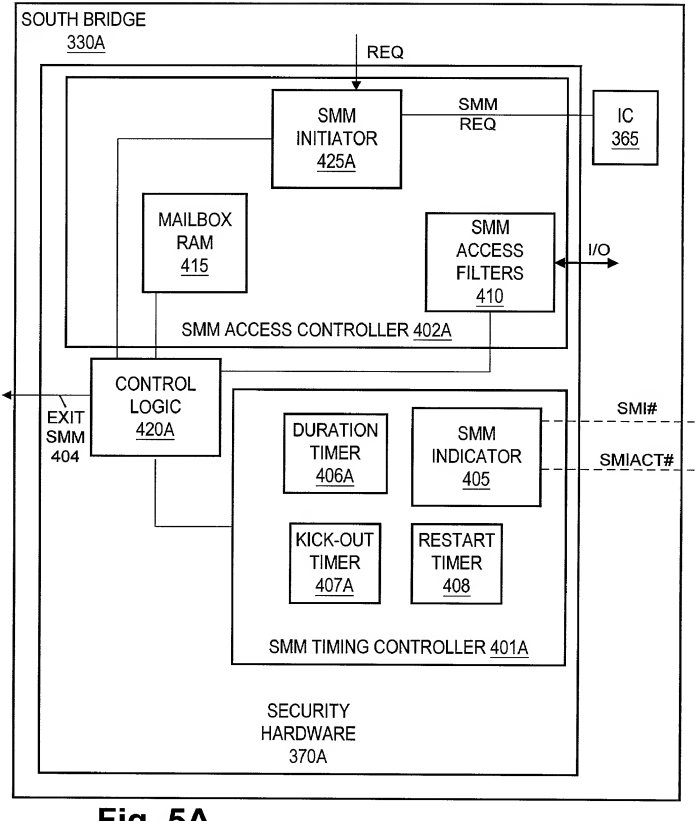

Fig. 5A

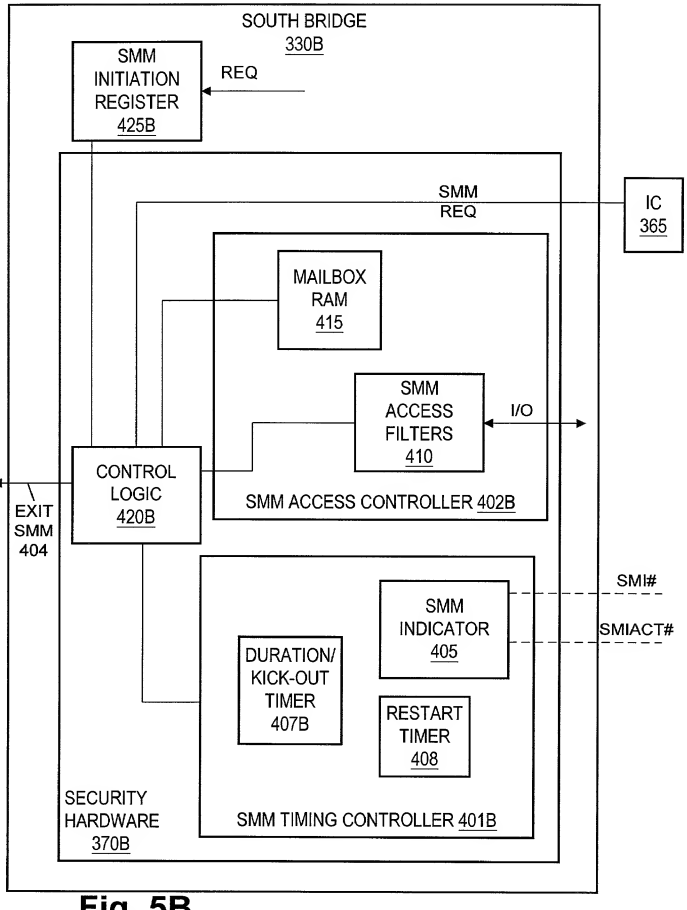
SOUTH BRIDGE
330B
SMM
INITIATION
REGISTER
425B
REQ
SMM
REQ
IC
365
MAILBOX
RAM
415
SMM
ACCESS
FILTERS
410
I/O
CONTROL
LOGIC
420B
SMM ACCESS CONTROLLER 402B
EXIT
SMM
404
SMI#
SMM
INDICATOR
405
SMIACT#
DURATION/
KICK-OUT
TIMER
407B
RESTART
TIMER
408
SECURITY
HARDWARE
370B
SMM TIMING CONTROLLER 401B

Fig. 5B

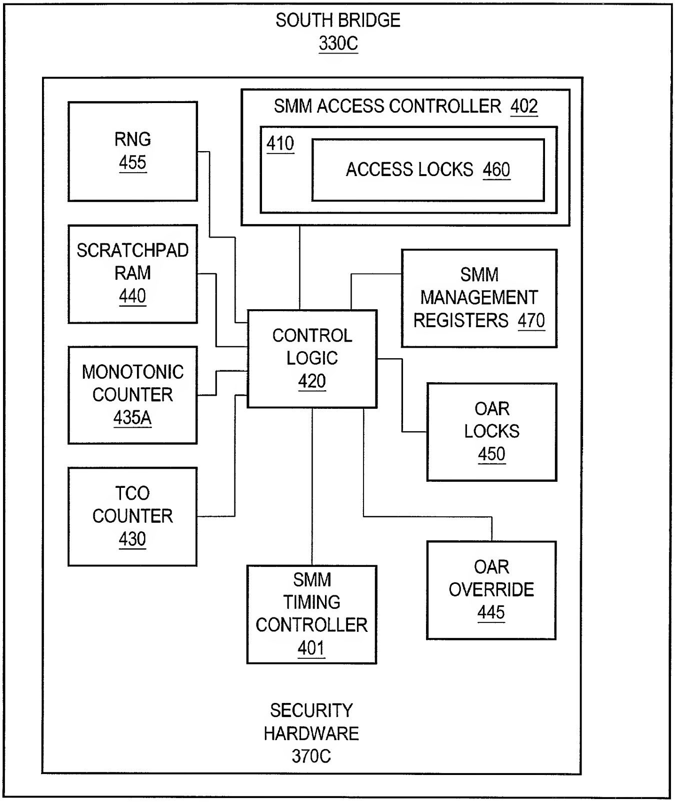

Fig. 6

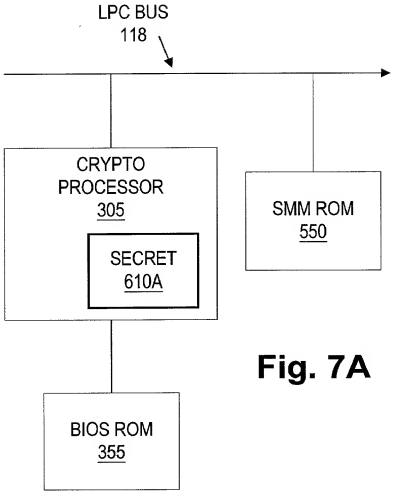

Fig. 7A

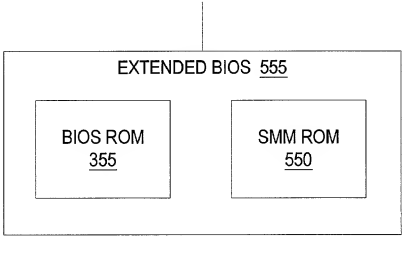

Fig. 7B

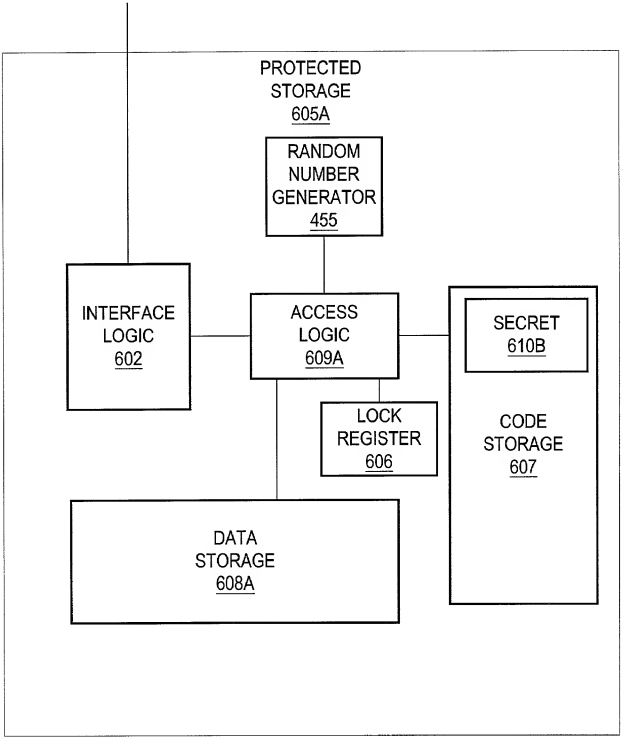
PROTECTED
STORAGE
605A
RANDOM
NUMBER
GENERATOR
455
INTERFACE
LOGIC
602
ACCESS
LOGIC
609A
SECRET
610B
LOCK
REGISTER
606
CODE
STORAGE
607
DATA
STORAGE
608A

Fig. 7C

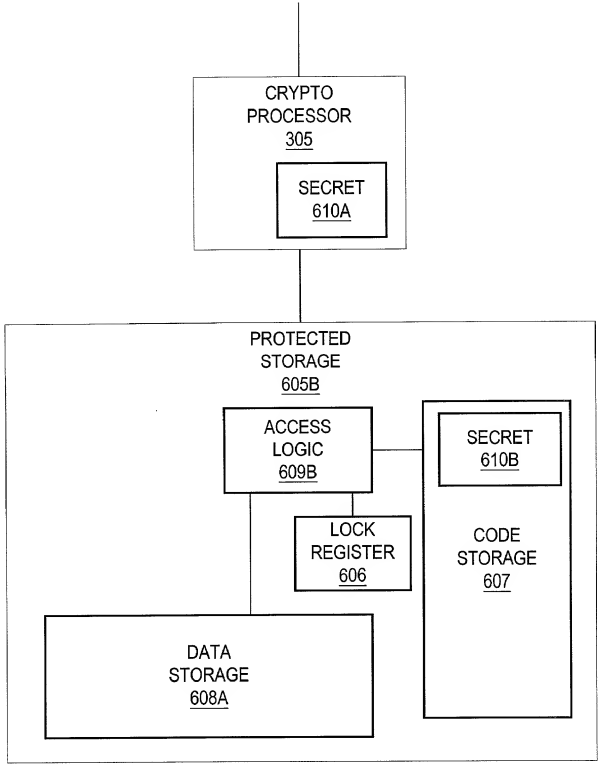

Fig. 7D

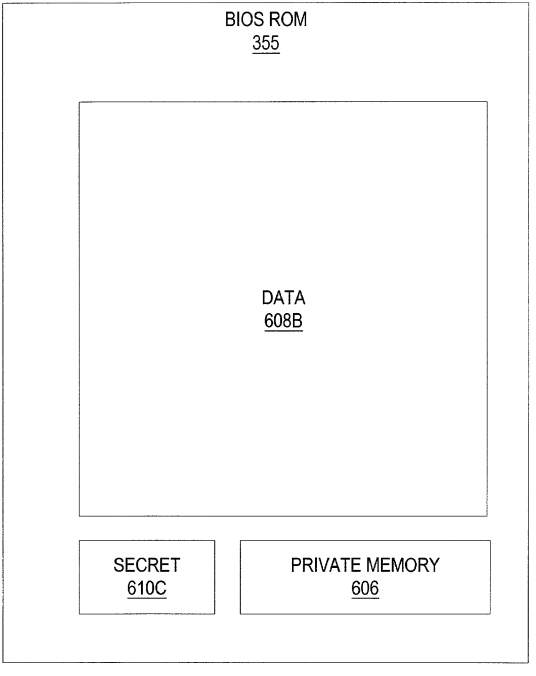

Fig. 8A

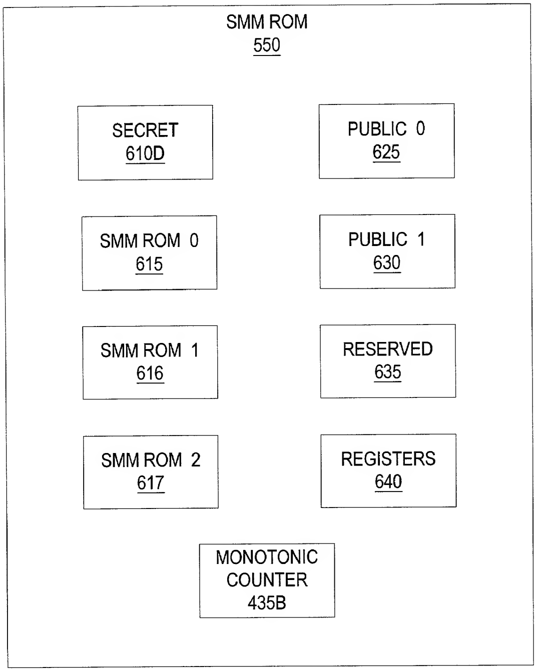
SMM ROM
550
SECRET
610D
PUBLIC 0
625
SMM ROM 0
615
PUBLIC 1
630
SMM ROM 1
616
RESERVED
635
SMM ROM 2
617
REGISTERS
640
MONOTONIC
COUNTER
435B

Fig. 8B

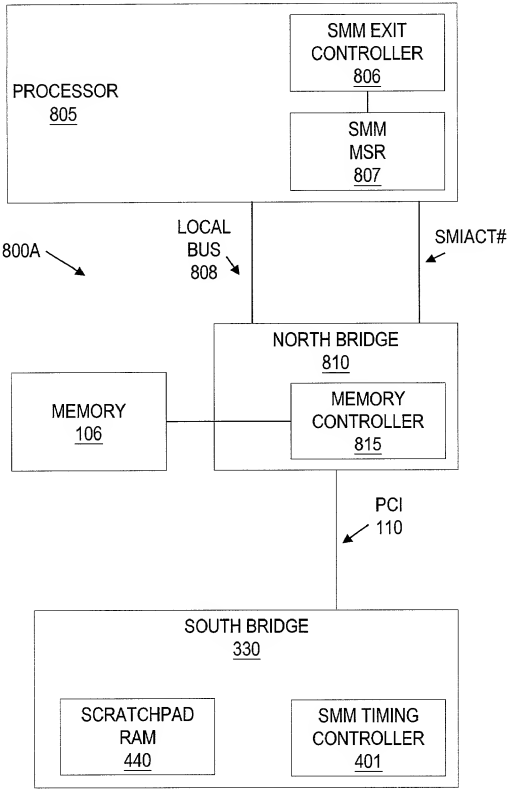

Fig. 9A

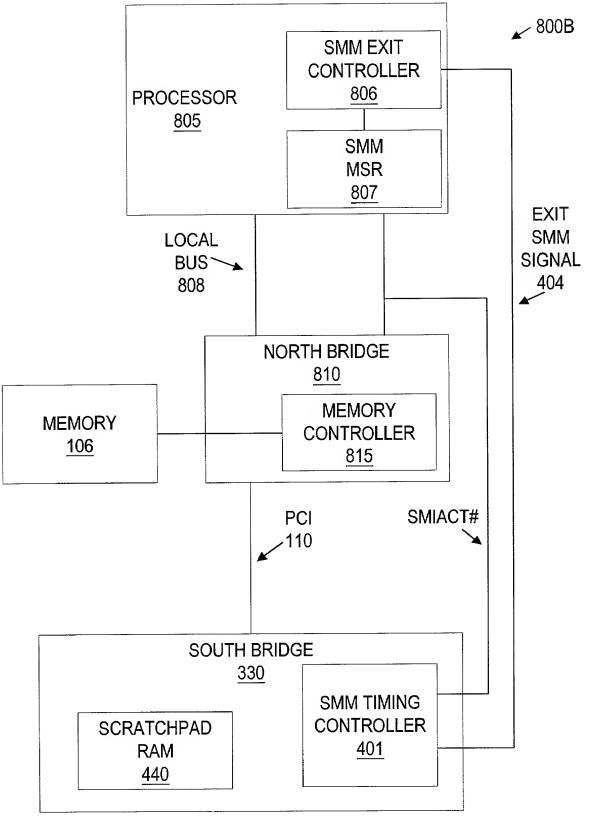
800B
SMM EXIT CONTROLLER 806
PROCESSOR 805
SMM MSR 807
EXIT SMM SIGNAL 404
LOCAL BUS 808
NORTH BRIDGE 810
MEMORY 106
MEMORY CONTROLLER 815
PCI 110
SMIACT#
SOUTH BRIDGE 330
SMM TIMING CONTROLLER 401
SCRATCHPAD RAM 440

Fig. 9B

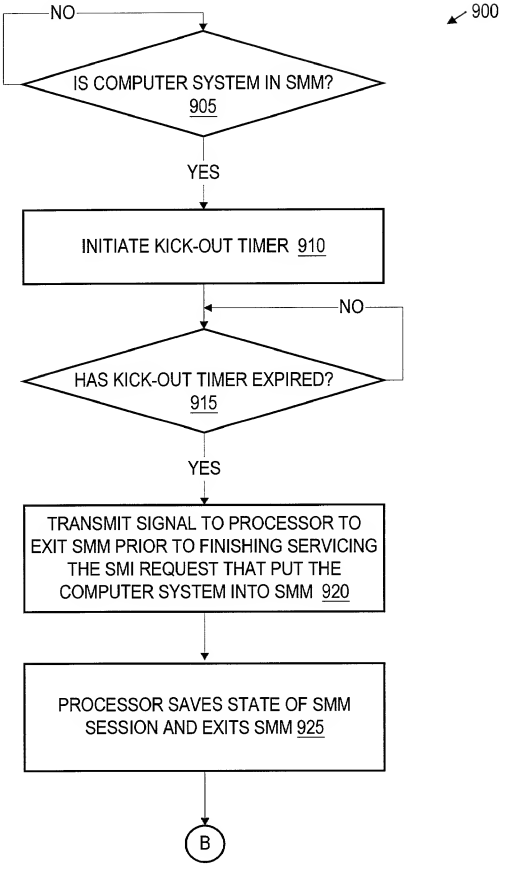

Fig. 10A

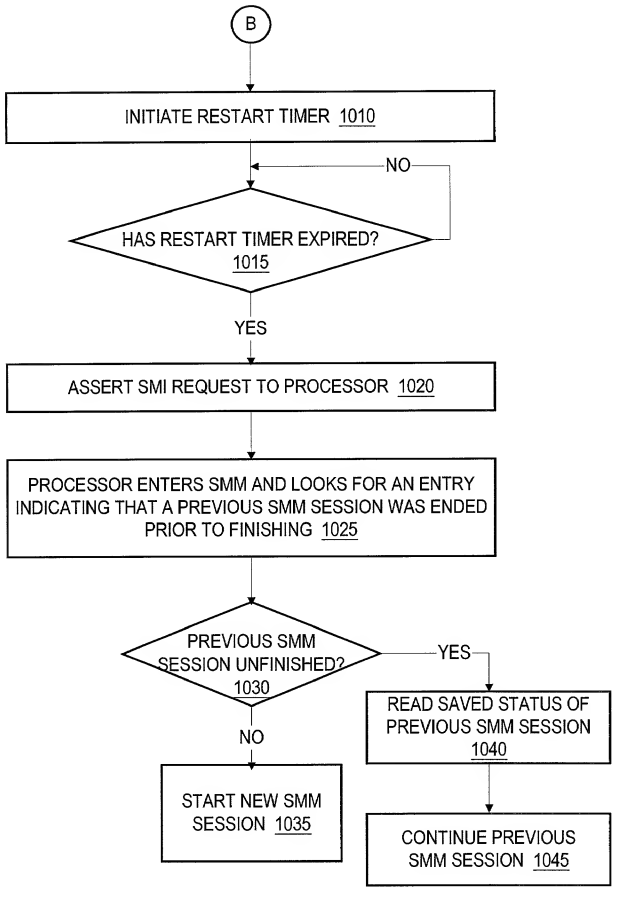

Fig. 10B

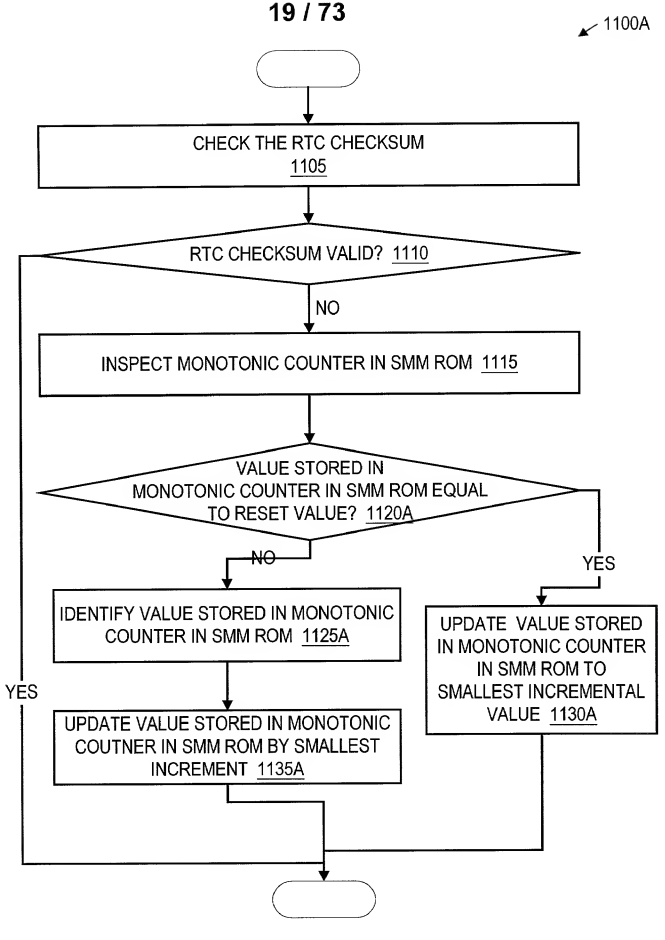

Fig. 11A

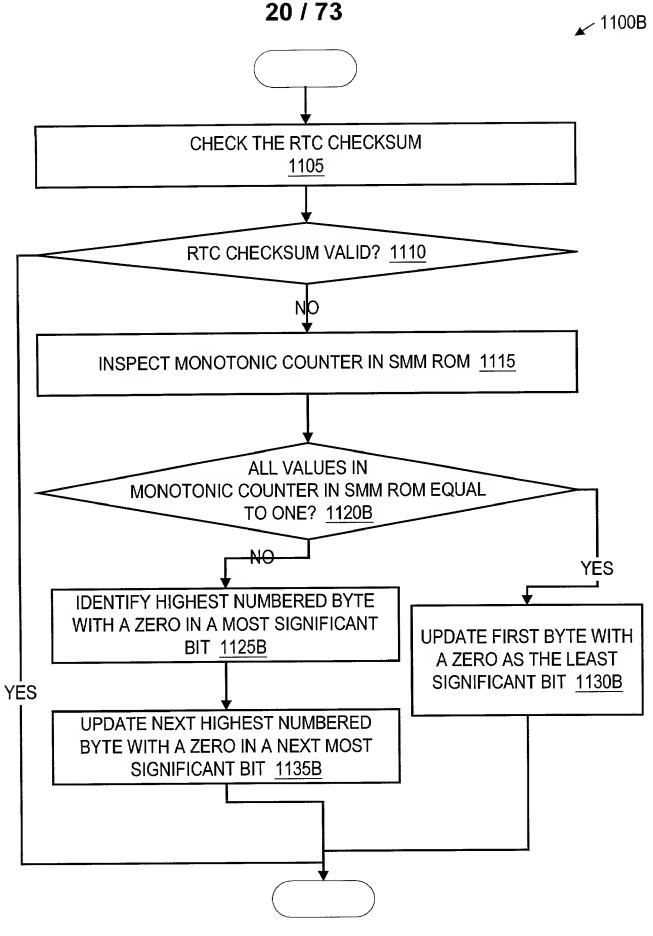

Fig. 11B

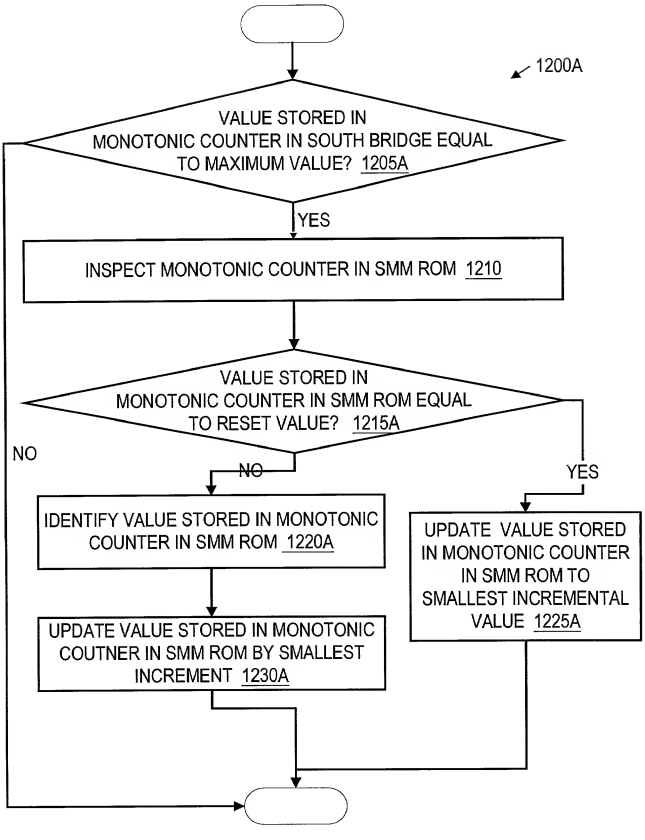
1200A
VALUE STORED IN MONOTONIC COUNTER IN SOUTH BRIDGE EQUAL TO MAXIMUM VALUE? 1205A
YES
INSPECT MONOTONIC COUNTER IN SMM ROM 1210
VALUE STORED IN MONOTONIC COUNTER IN SMM ROM EQUAL TO RESET VALUE? 1215A
NO
NO
YES
IDENTIFY VALUE STORED IN MONOTONIC COUNTER IN SMM ROM 1220A
UPDATE VALUE STORED IN MONOTONIC COUTNER IN SMM ROM BY SMALLEST INCREMENT 1230A
UPDATE VALUE STORED IN MONOTONIC COUNTER IN SMM ROM TO SMALLEST INCREMENTAL VALUE 1225A

Fig. 12A

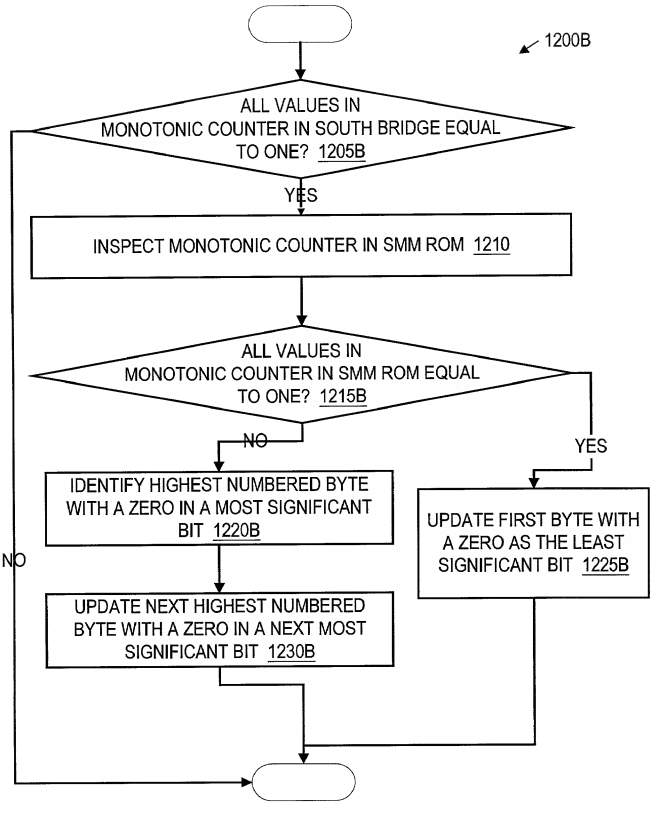
1200B
ALL VALUES IN MONOTONIC COUNTER IN SOUTH BRIDGE EQUAL TO ONE? 1205B
YES
INSPECT MONOTONIC COUNTER IN SMM ROM 1210
ALL VALUES IN MONOTONIC COUNTER IN SMM ROM EQUAL TO ONE? 1215B
NO
YES
IDENTIFY HIGHEST NUMBERED BYTE WITH A ZERO IN A MOST SIGNIFICANT BIT 1220B
UPDATE FIRST BYTE WITH A ZERO AS THE LEAST SIGNIFICANT BIT 1225B
NO
UPDATE NEXT HIGHEST NUMBERED BYTE WITH A ZERO IN A NEXT MOST SIGNIFICANT BIT 1230B

Fig. 12B

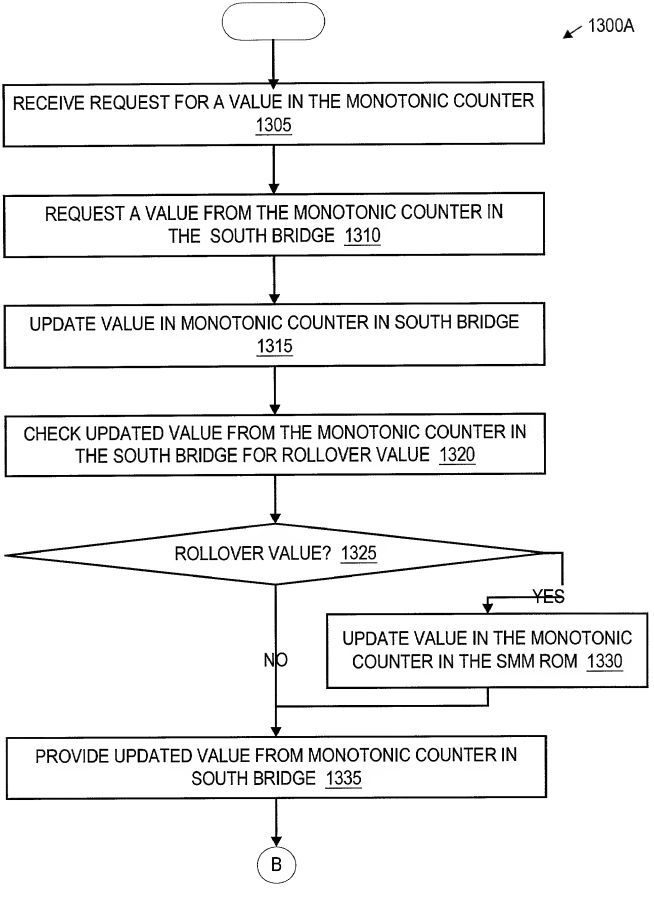

Fig. 13A

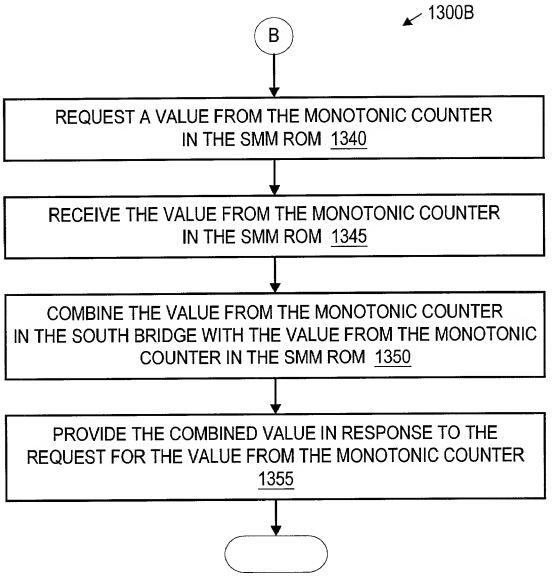

Fig. 13B

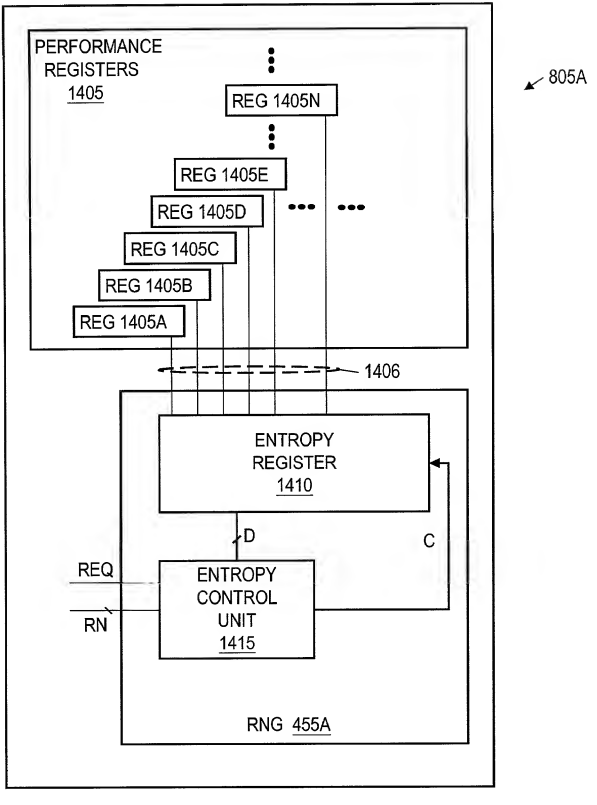

Fig. 14A

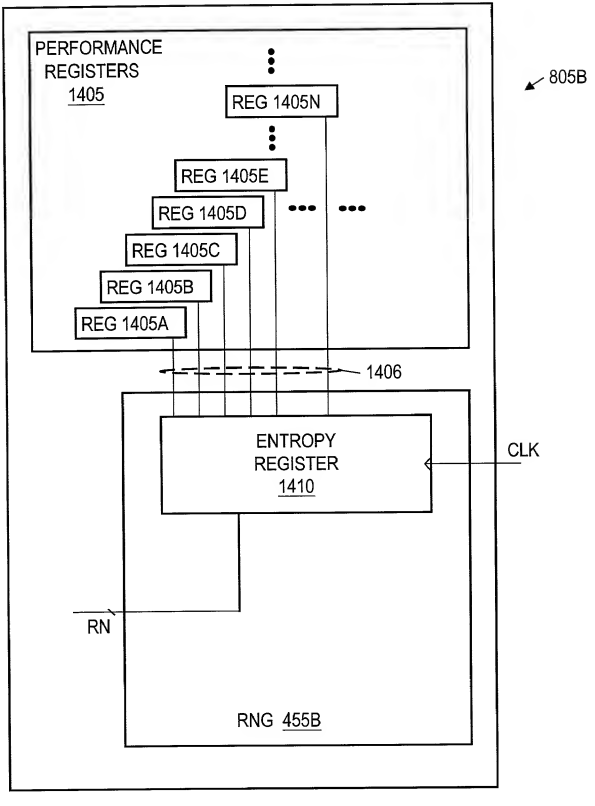
PERFORMANCE
REGISTERS
1405
805B
REG 1405N
REG 1405E
REG 1405D
REG 1405C
REG 1405B
REG 1405A
1406
ENTROPY
REGISTER
1410
CLK
RN
RNG 455B

Fig. 14B

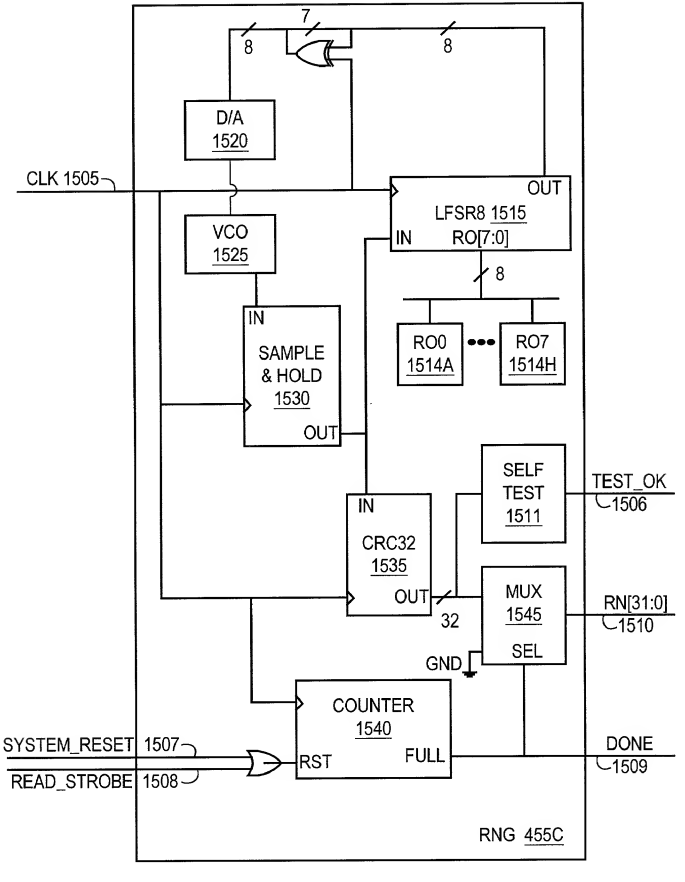
7
8
8
D/A
1520
CLK 1505
OUT
LFSR8 1515
IN
RO[7:0]
VCO
1525
8
IN
SAMPLE
& HOLD
1530
OUT
RO0
1514A
RO7
1514H
SELF
TEST
1511
TEST_OK
1506
IN
CRC32
1535
OUT
32
MUX
1545
SEL
RN[31:0]
1510
GND
COUNTER
1540
SYSTEM_RESET 1507
READ_STROBE 1508
RST
FULL
DONE
1509
RNG 455C

Fig. 15

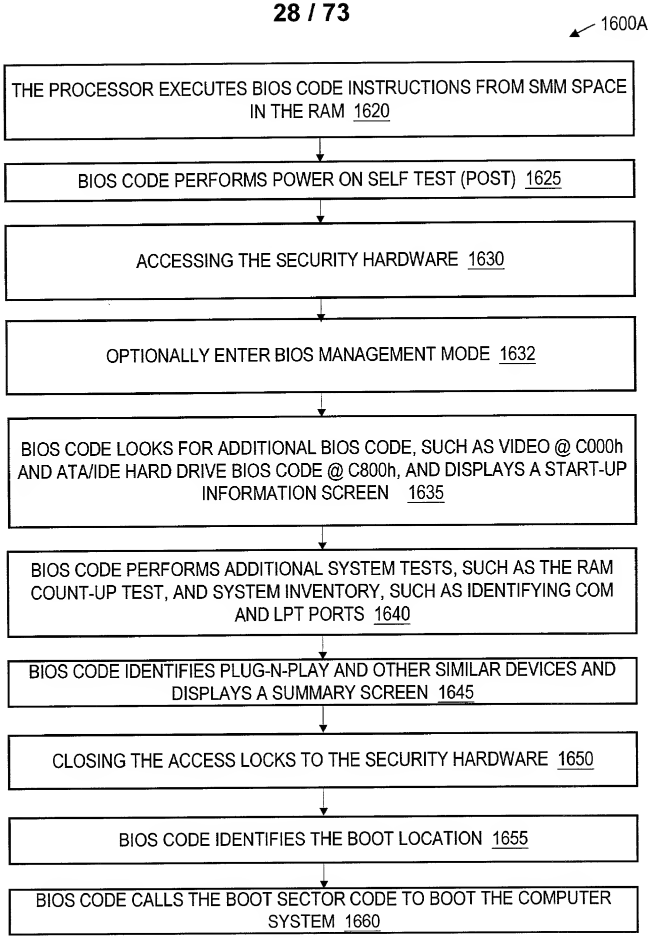
1600A
THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE IN THE RAM 1620
BIOS CODE PERFORMS POWER ON SELF TEST (POST) 1625
ACCESSING THE SECURITY HARDWARE 1630
OPTIONALLY ENTER BIOS MANAGEMENT MODE 1632
BIOS CODE LOOKS FOR ADDITIONAL BIOS CODE, SUCH AS VIDEO @ C000h AND ATA/IDE HARD DRIVE BIOS CODE @ C800h, AND DISPLAYS A START-UP INFORMATION SCREEN 1635
BIOS CODE PERFORMS ADDITIONAL SYSTEM TESTS, SUCH AS THE RAM COUNT-UP TEST, AND SYSTEM INVENTORY, SUCH AS IDENTIFYING COM AND LPT PORTS 1640
BIOS CODE IDENTIFIES PLUG-N-PLAY AND OTHER SIMILAR DEVICES AND DISPLAYS A SUMMARY SCREEN 1645
CLOSING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1650
BIOS CODE IDENTIFIES THE BOOT LOCATION 1655
BIOS CODE CALLS THE BOOT SECTOR CODE TO BOOT THE COMPUTER SYSTEM 1660

Fig. 16A

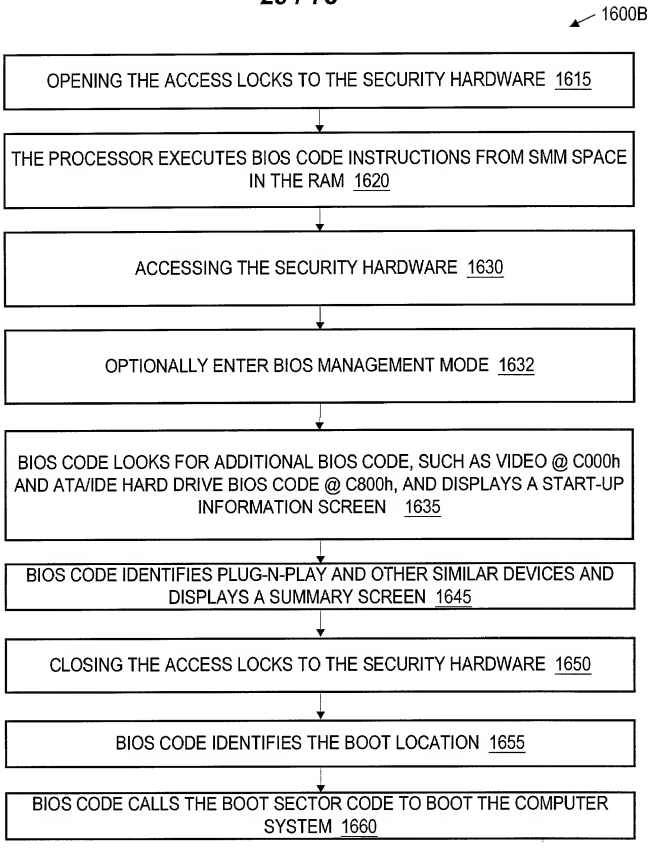
1600B
OPENING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1615
THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE IN THE RAM 1620
ACCESSING THE SECURITY HARDWARE 1630
OPTIONALLY ENTER BIOS MANAGEMENT MODE 1632
BIOS CODE LOOKS FOR ADDITIONAL BIOS CODE, SUCH AS VIDEO @ C000h AND ATA/IDE HARD DRIVE BIOS CODE @ C800h, AND DISPLAYS A START-UP INFORMATION SCREEN 1635
BIOS CODE IDENTIFIES PLUG-N-PLAY AND OTHER SIMILAR DEVICES AND DISPLAYS A SUMMARY SCREEN 1645
CLOSING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1650
BIOS CODE IDENTIFIES THE BOOT LOCATION 1655
BIOS CODE CALLS THE BOOT SECTOR CODE TO BOOT THE COMPUTER SYSTEM 1660

Fig. 16B

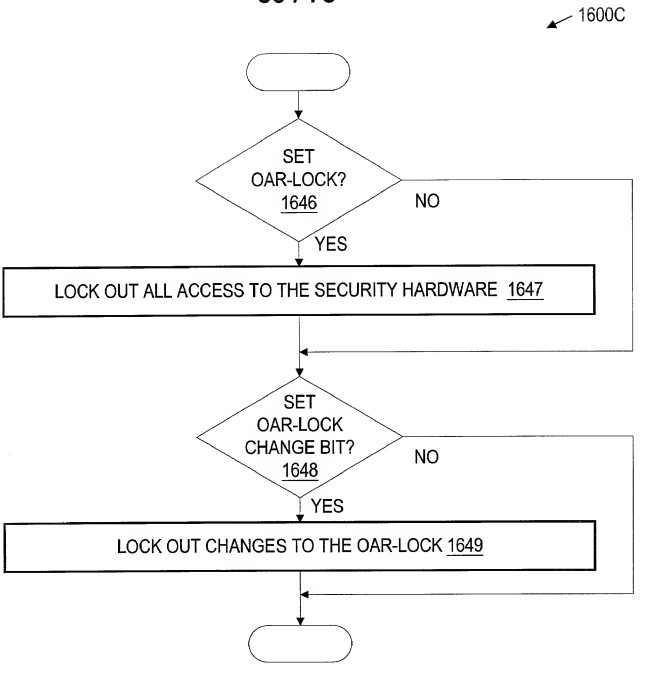

Fig. 16C

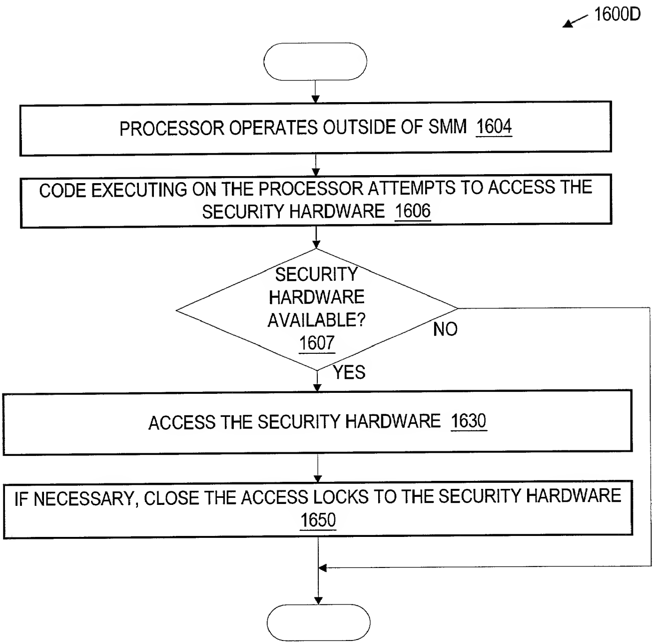
1600D
PROCESSOR OPERATES OUTSIDE OF SMM 1604
CODE EXECUTING ON THE PROCESSOR ATTEMPTS TO ACCESS THE SECURITY HARDWARE 1606
SECURITY HARDWARE AVAILABLE? 1607
NO
YES
ACCESS THE SECURITY HARDWARE 1630
IF NECESSARY, CLOSE THE ACCESS LOCKS TO THE SECURITY HARDWARE 1650

Fig. 16D

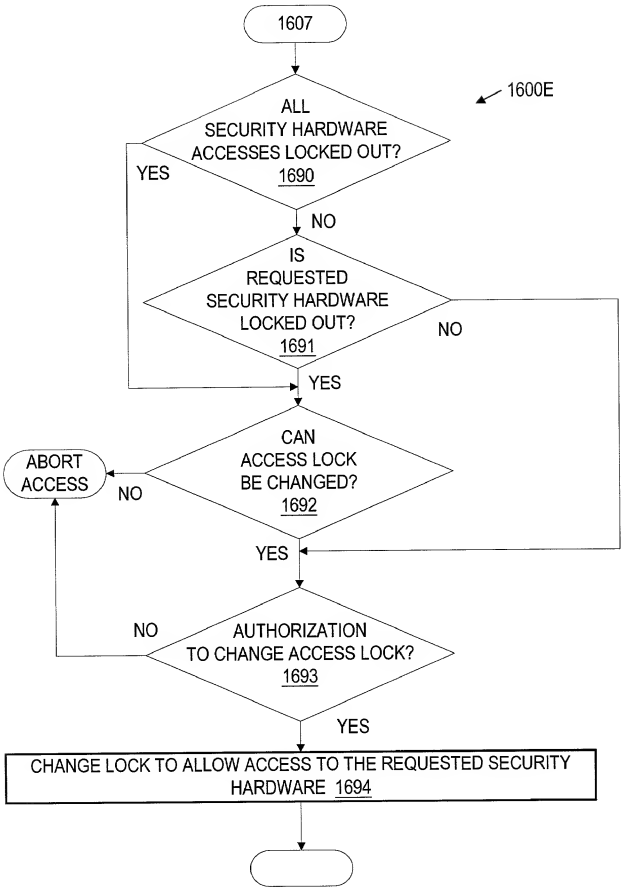

Fig. 16E

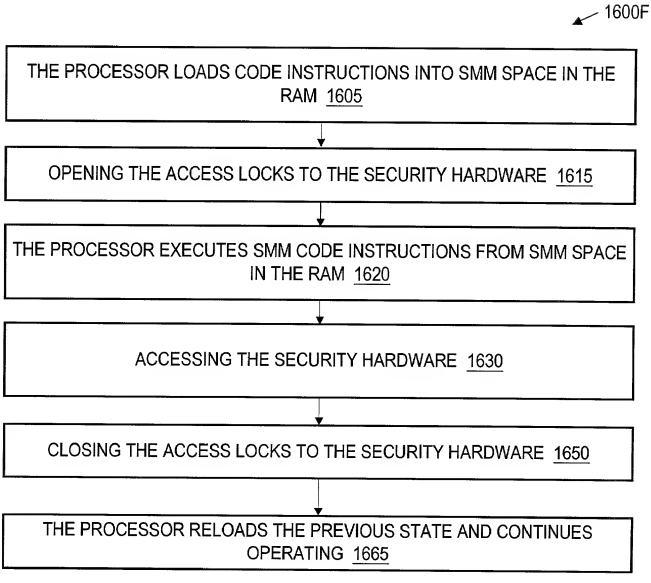

Fig. 16F

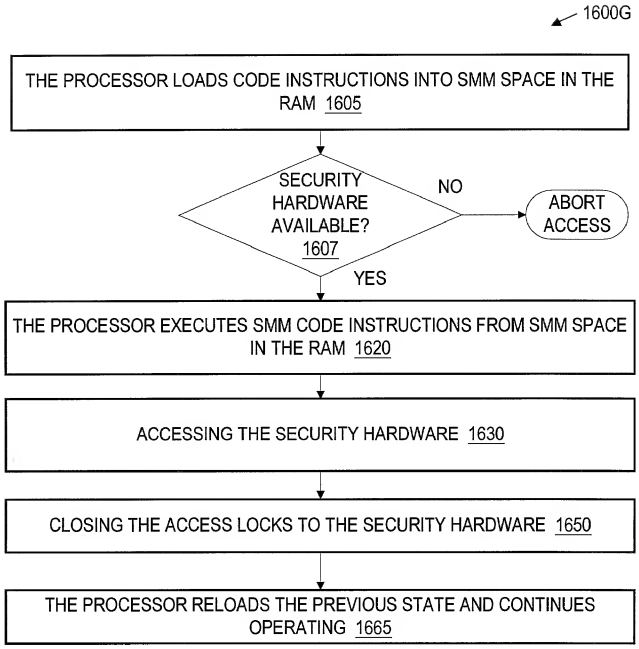

Fig. 16G

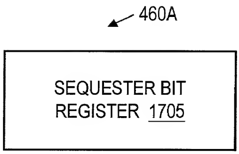

Fig. 17A

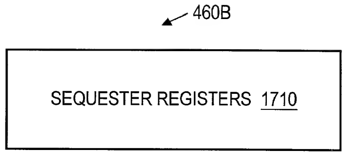

Fig. 17B

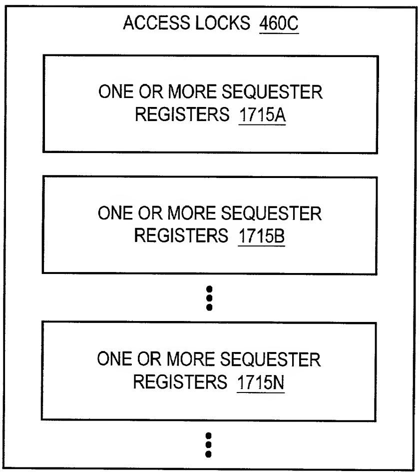

Fig. 17C

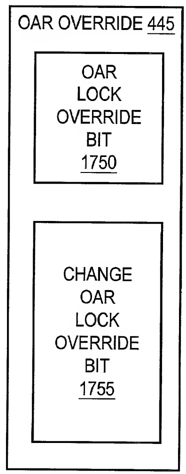

Fig. 17D

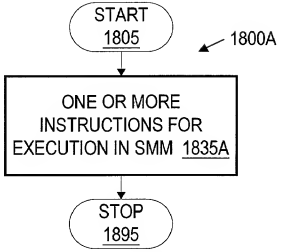

Fig. 18A
PRIOR ART

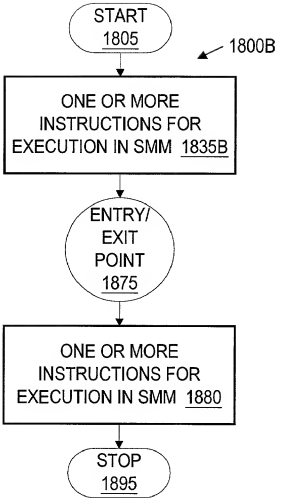

Fig. 18B

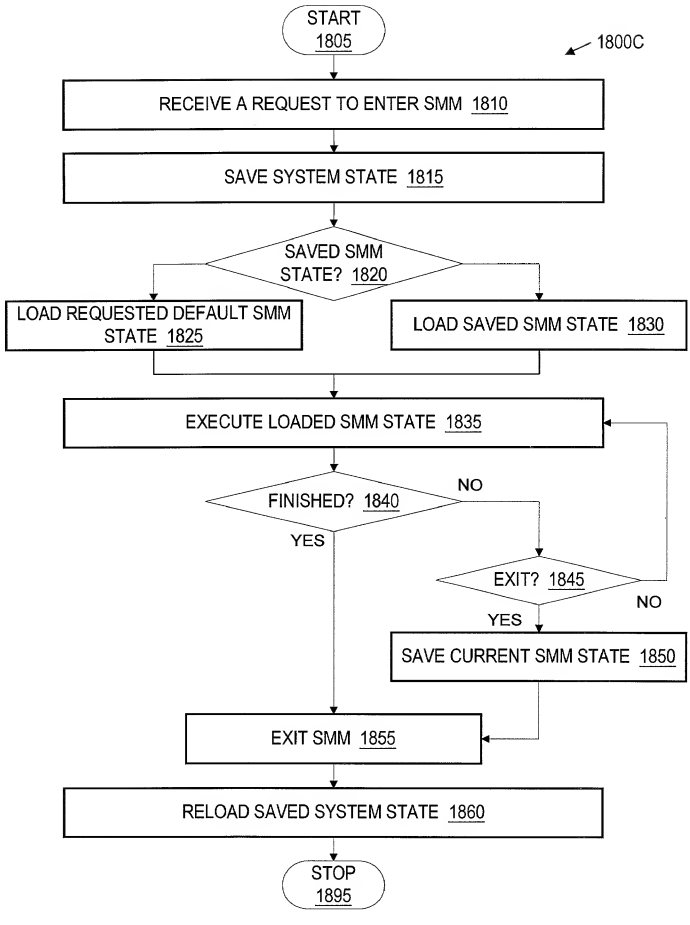

Fig. 18C

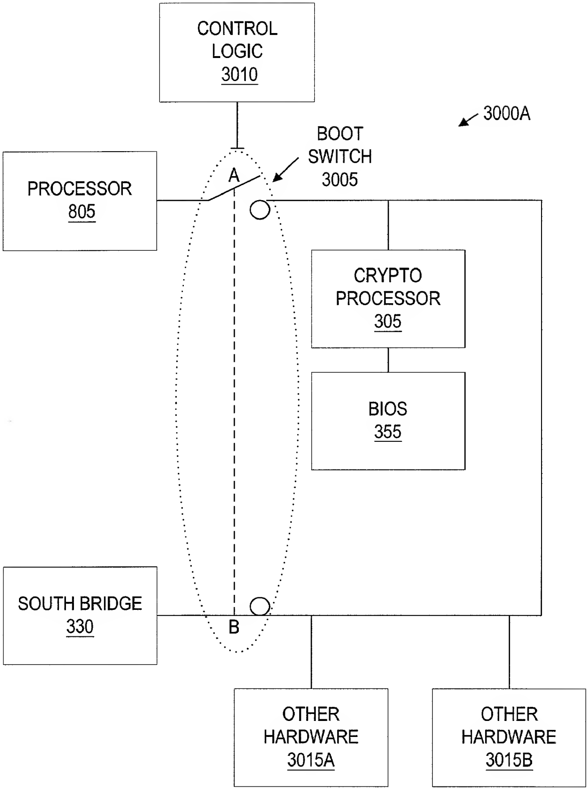
CONTROL
LOGIC
3010
3000A
BOOT
SWITCH
3005
PROCESSOR
805
A
CRYPTO
PROCESSOR
305
BIOS
355
SOUTH BRIDGE
330
B
OTHER
HARDWARE
3015A
OTHER
HARDWARE
3015B

Fig. 19A

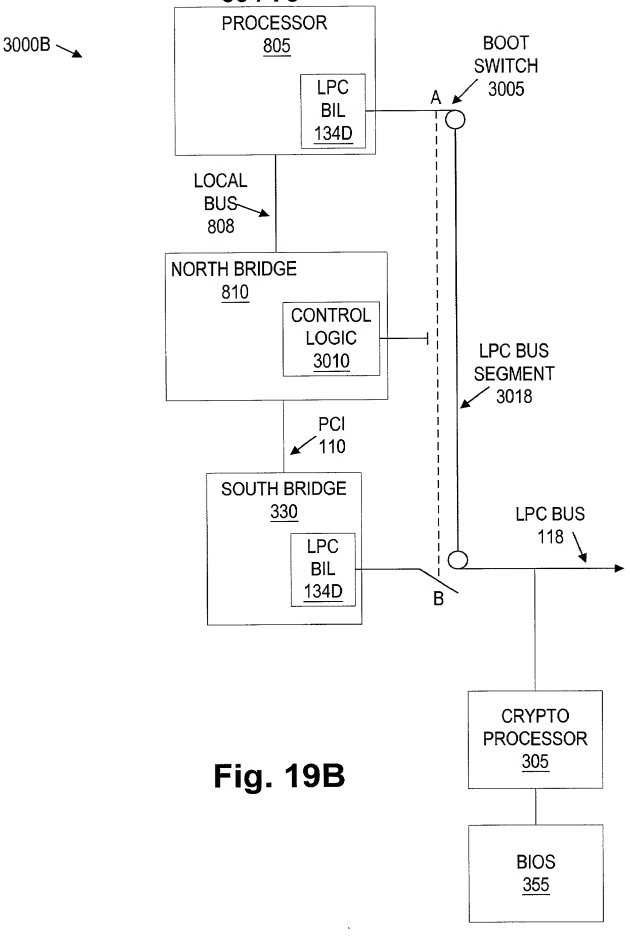

Fig. 19B

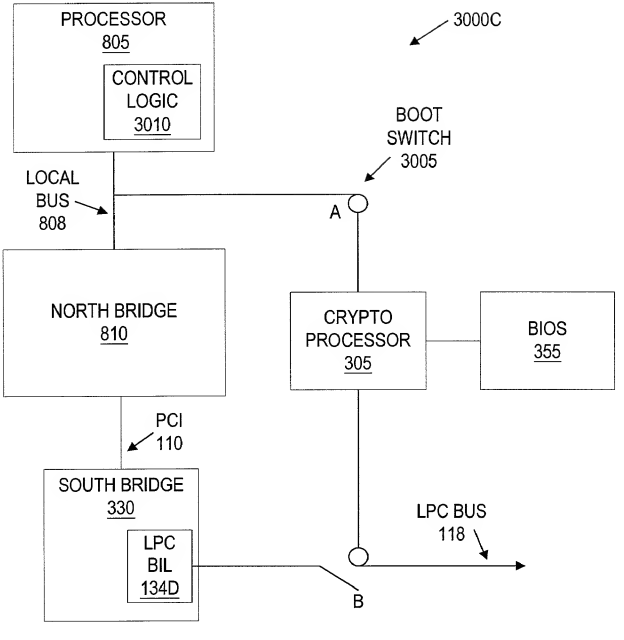

Fig. 19C

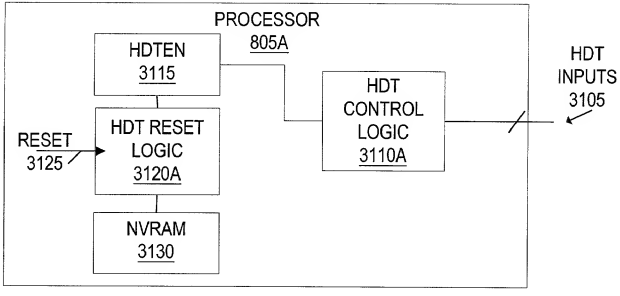

Fig. 20A

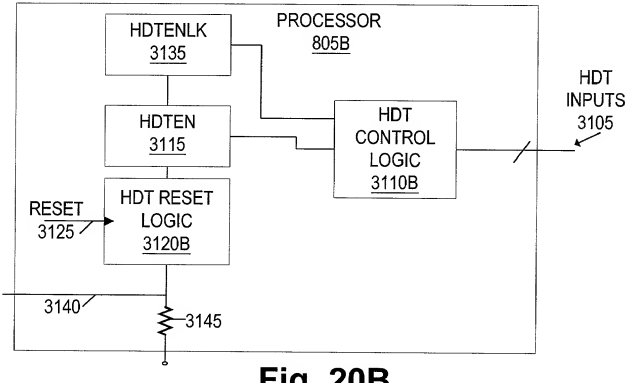

Fig. 20B

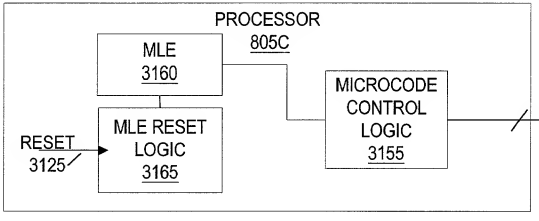

Fig. 20C

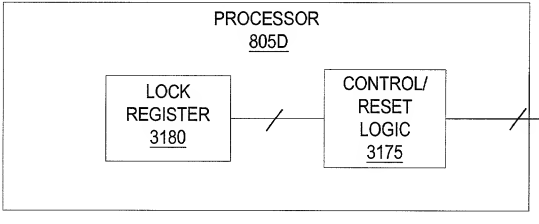

Fig. 20D

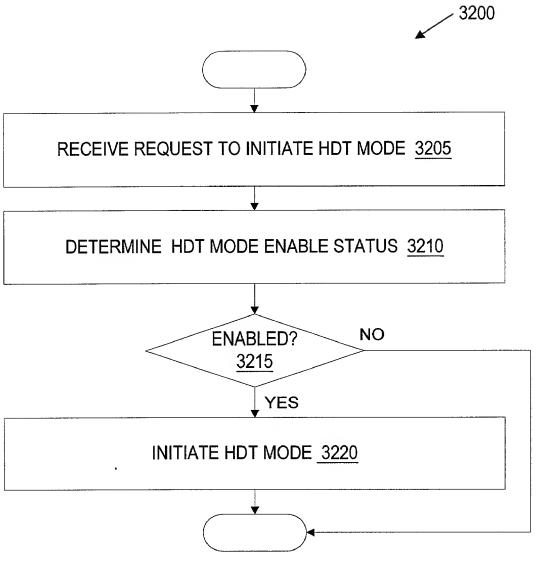

Fig. 21

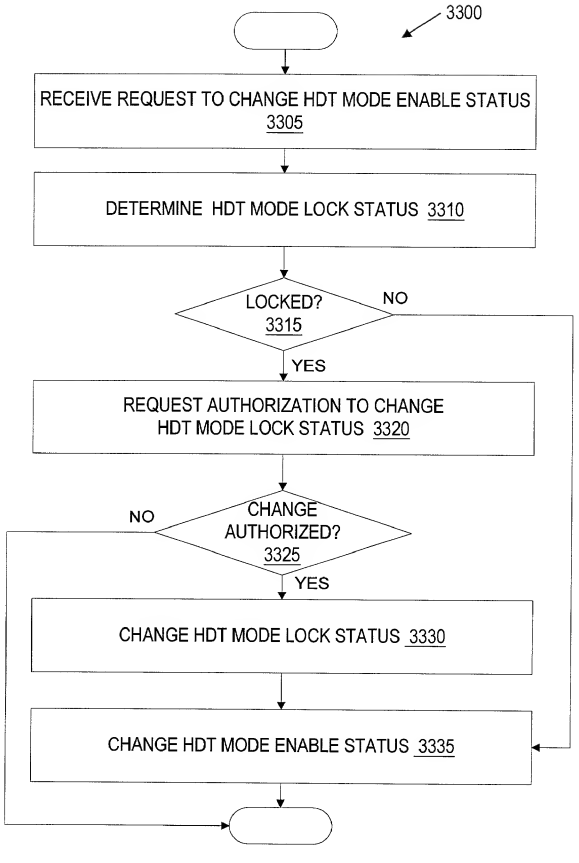

Fig. 22

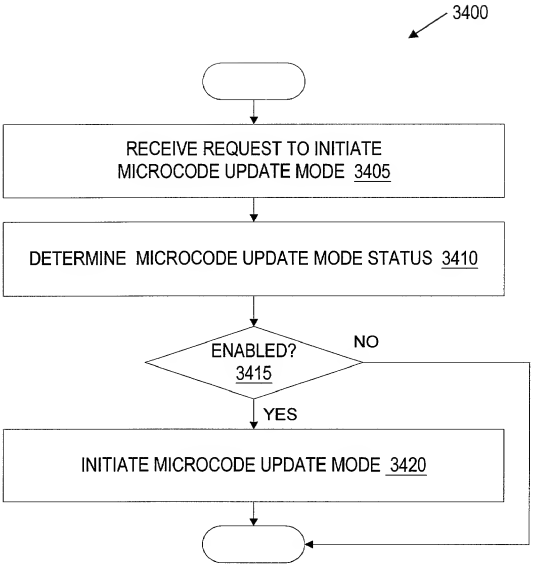

Fig. 23

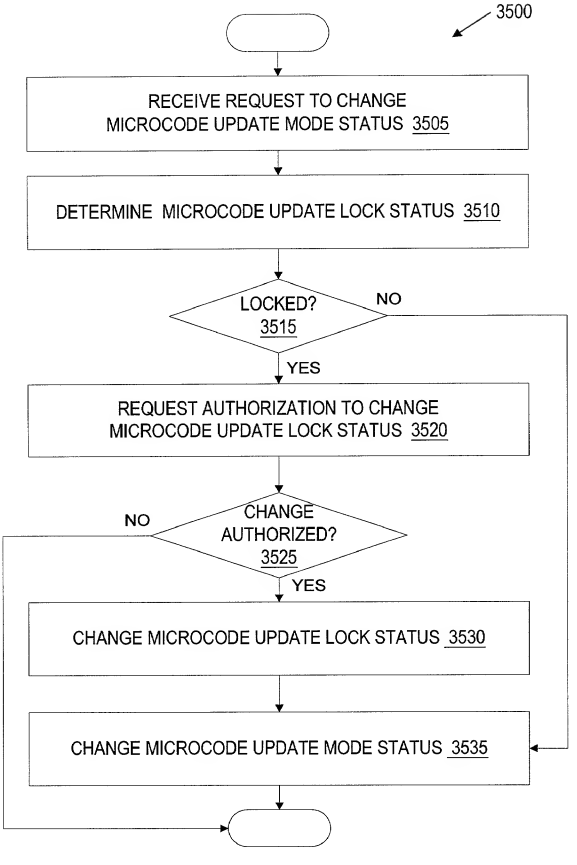

Fig. 24

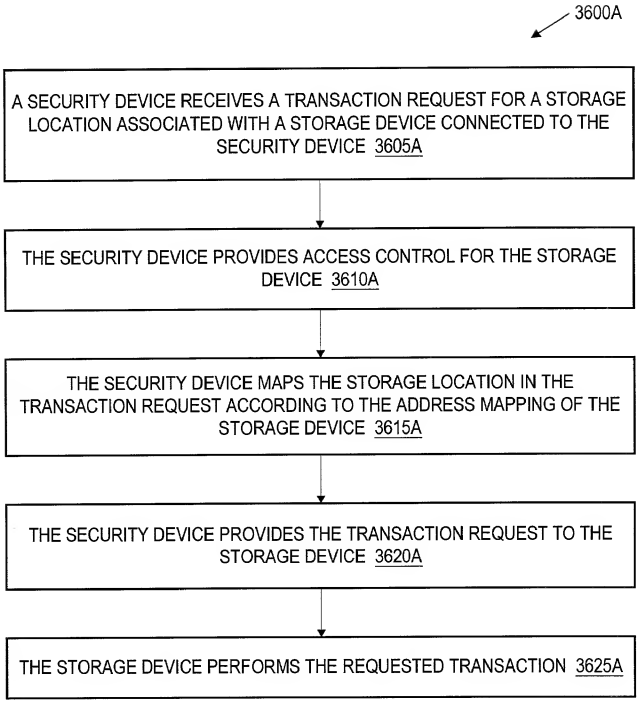
3600A
A SECURITY DEVICE RECEIVES A TRANSACTION REQUEST FOR A STORAGE LOCATION ASSOCIATED WITH A STORAGE DEVICE CONNECTED TO THE SECURITY DEVICE 3605A
THE SECURITY DEVICE PROVIDES ACCESS CONTROL FOR THE STORAGE DEVICE 3610A
THE SECURITY DEVICE MAPS THE STORAGE LOCATION IN THE TRANSACTION REQUEST ACCORDING TO THE ADDRESS MAPPING OF THE STORAGE DEVICE 3615A
THE SECURITY DEVICE PROVIDES THE TRANSACTION REQUEST TO THE STORAGE DEVICE 3620A
THE STORAGE DEVICE PERFORMS THE REQUESTED TRANSACTION 3625A

Fig. 25A

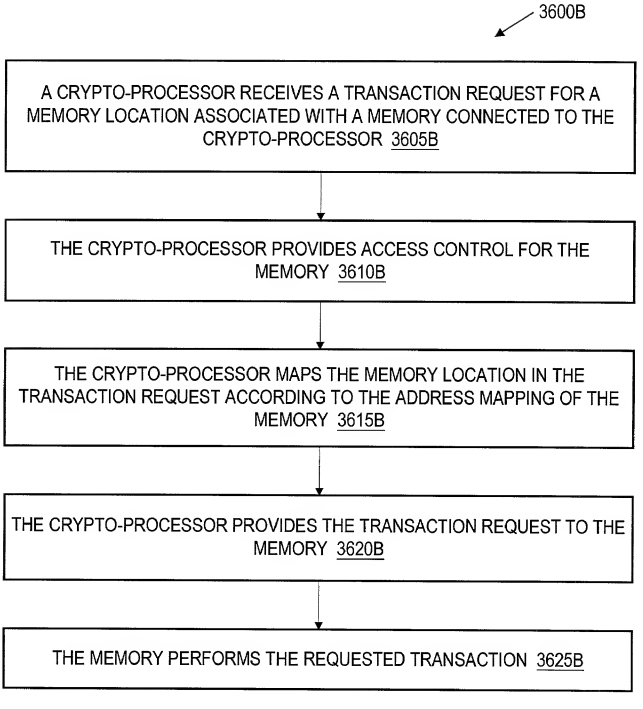
3600B
A CRYPTO-PROCESSOR RECEIVES A TRANSACTION REQUEST FOR A MEMORY LOCATION ASSOCIATED WITH A MEMORY CONNECTED TO THE CRYPTO-PROCESSOR 3605B
THE CRYPTO-PROCESSOR PROVIDES ACCESS CONTROL FOR THE MEMORY 3610B
THE CRYPTO-PROCESSOR MAPS THE MEMORY LOCATION IN THE TRANSACTION REQUEST ACCORDING TO THE ADDRESS MAPPING OF THE MEMORY 3615B
THE CRYPTO-PROCESSOR PROVIDES THE TRANSACTION REQUEST TO THE MEMORY 3620B
THE MEMORY PERFORMS THE REQUESTED TRANSACTION 3625B

Fig. 25B

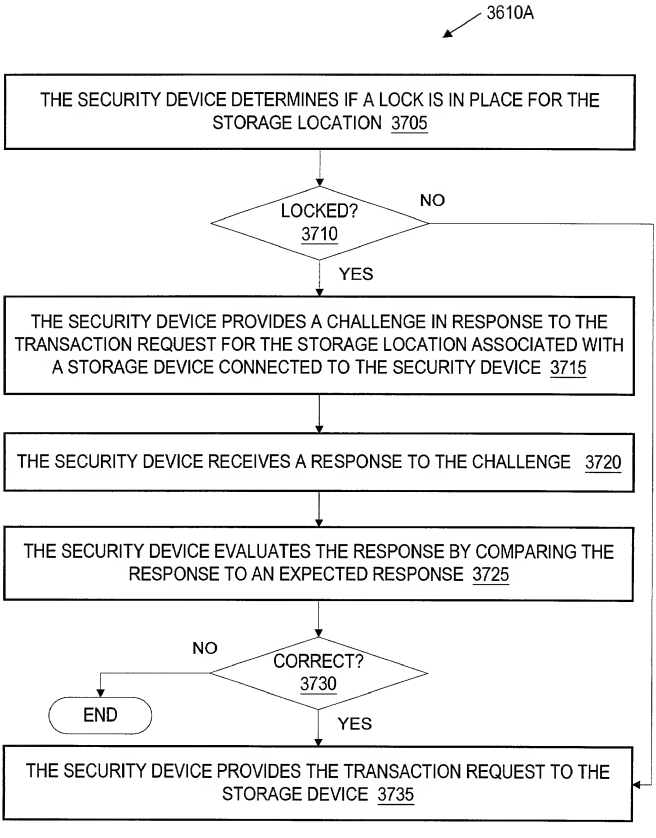
3610A
THE SECURITY DEVICE DETERMINES IF A LOCK IS IN PLACE FOR THE STORAGE LOCATION 3705
LOCKED? 3710
NO
YES
THE SECURITY DEVICE PROVIDES A CHALLENGE IN RESPONSE TO THE TRANSACTION REQUEST FOR THE STORAGE LOCATION ASSOCIATED WITH A STORAGE DEVICE CONNECTED TO THE SECURITY DEVICE 3715
THE SECURITY DEVICE RECEIVES A RESPONSE TO THE CHALLENGE 3720
THE SECURITY DEVICE EVALUATES THE RESPONSE BY COMPARING THE RESPONSE TO AN EXPECTED RESPONSE 3725
NO
CORRECT? 3730
END
YES
THE SECURITY DEVICE PROVIDES THE TRANSACTION REQUEST TO THE STORAGE DEVICE 3735

Fig. 26

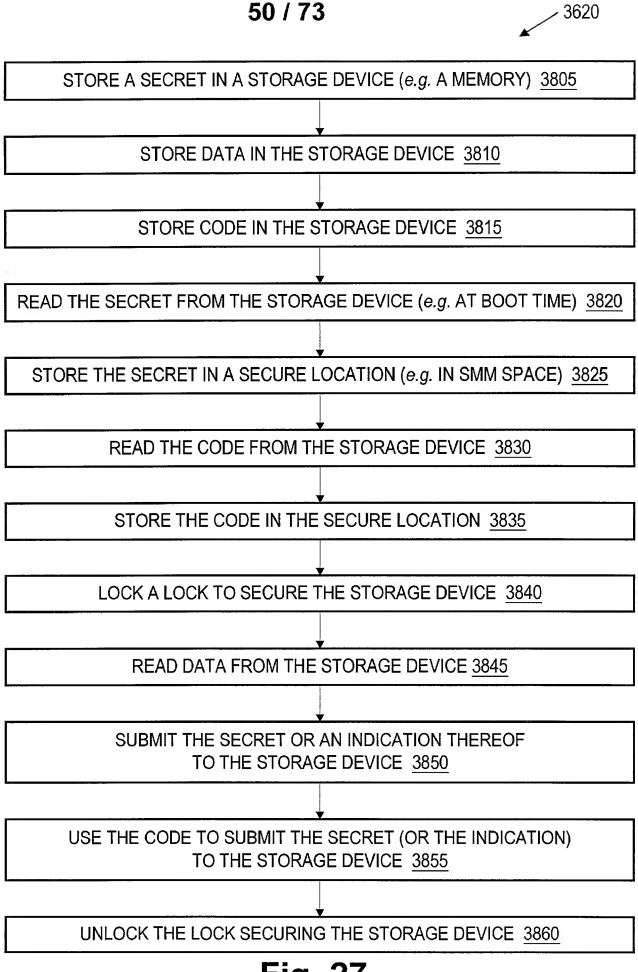

Fig. 27

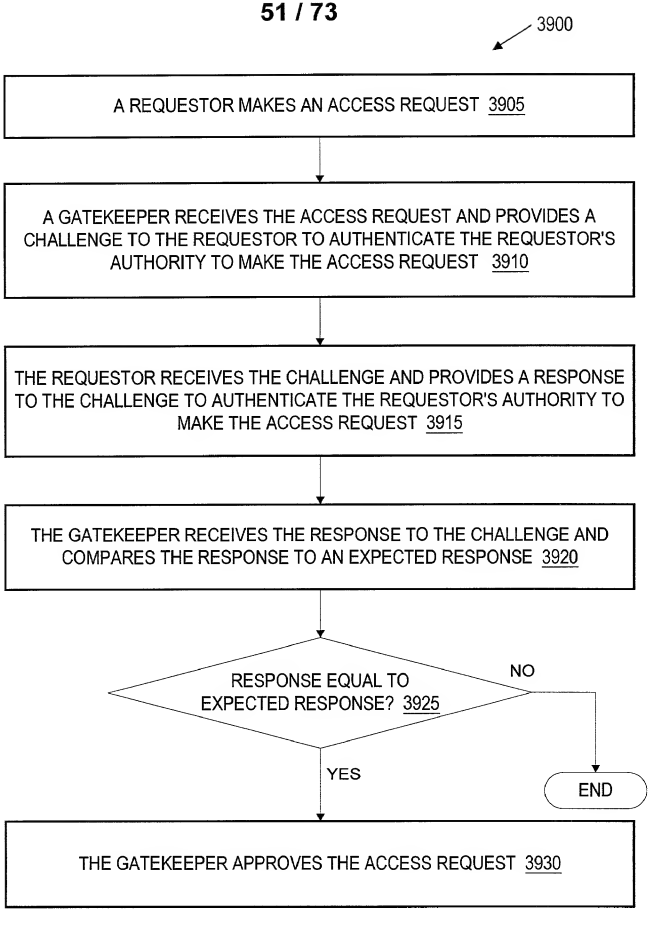

Fig. 28
(Prior Art)

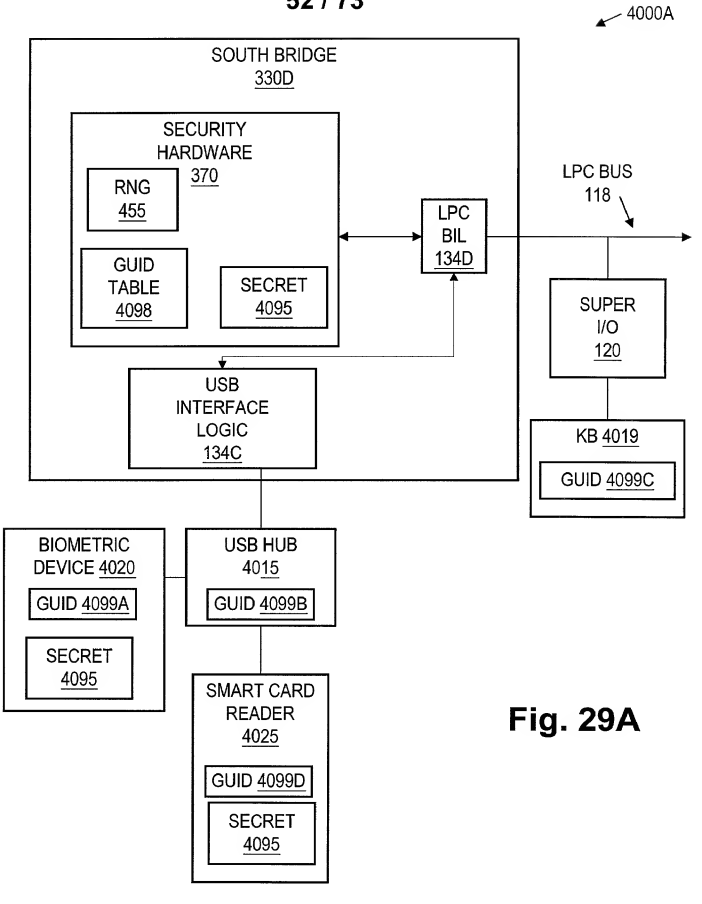

Fig. 29A

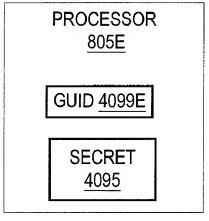

Fig. 29B

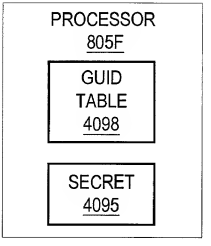

Fig. 29C

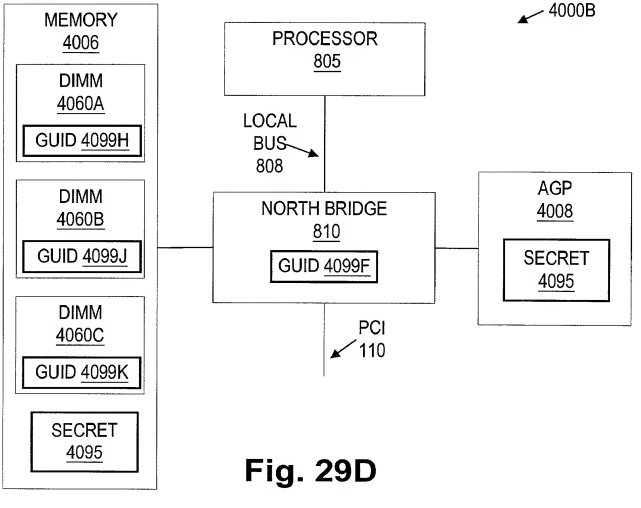

Fig. 29D

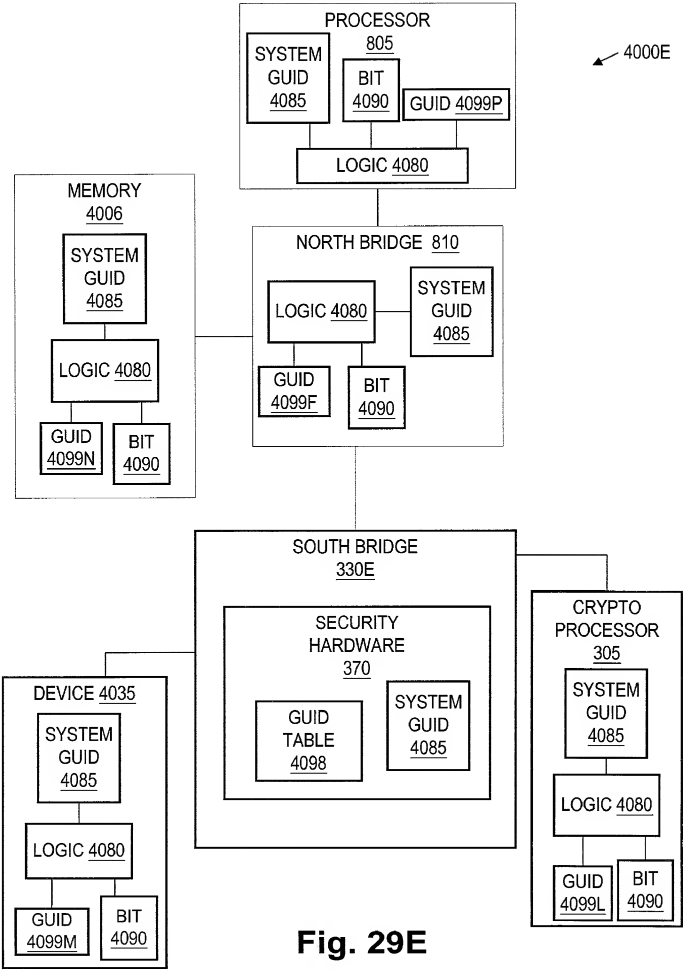
PROCESSOR
805
SYSTEM GUID 4085
BIT 4090
GUID 4099P
LOGIC 4080
4000E
MEMORY
4006
SYSTEM GUID 4085
LOGIC 4080
GUID 4099N
BIT 4090
NORTH BRIDGE 810
LOGIC 4080
SYSTEM GUID 4085
GUID 4099F
BIT 4090
SOUTH BRIDGE
330E
SECURITY HARDWARE
370
GUID TABLE 4098
SYSTEM GUID 4085
CRYPTO PROCESSOR
305
SYSTEM GUID 4085
LOGIC 4080
GUID 4099L
BIT 4090
DEVICE 4035
SYSTEM GUID 4085
LOGIC 4080
GUID 4099M
BIT 4090

Fig. 29E

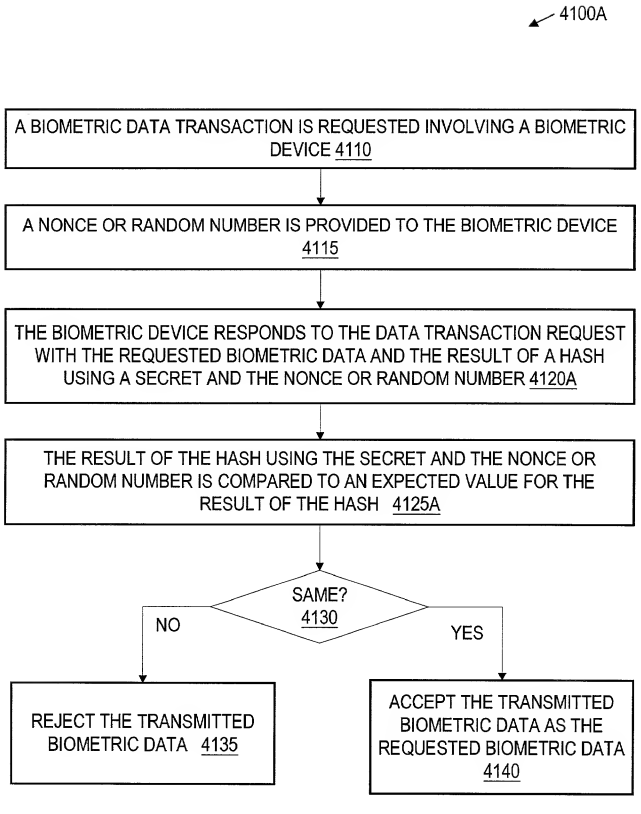
4100A
A BIOMETRIC DATA TRANSACTION IS REQUESTED INVOLVING A BIOMETRIC DEVICE 4110
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE BIOMETRIC DEVICE 4115
THE BIOMETRIC DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST WITH THE REQUESTED BIOMETRIC DATA AND THE RESULT OF A HASH USING A SECRET AND THE NONCE OR RANDOM NUMBER 4120A
THE RESULT OF THE HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4125A
SAME? 4130
NO
YES
REJECT THE TRANSMITTED BIOMETRIC DATA 4135
ACCEPT THE TRANSMITTED BIOMETRIC DATA AS THE REQUESTED BIOMETRIC DATA 4140

Fig. 30A

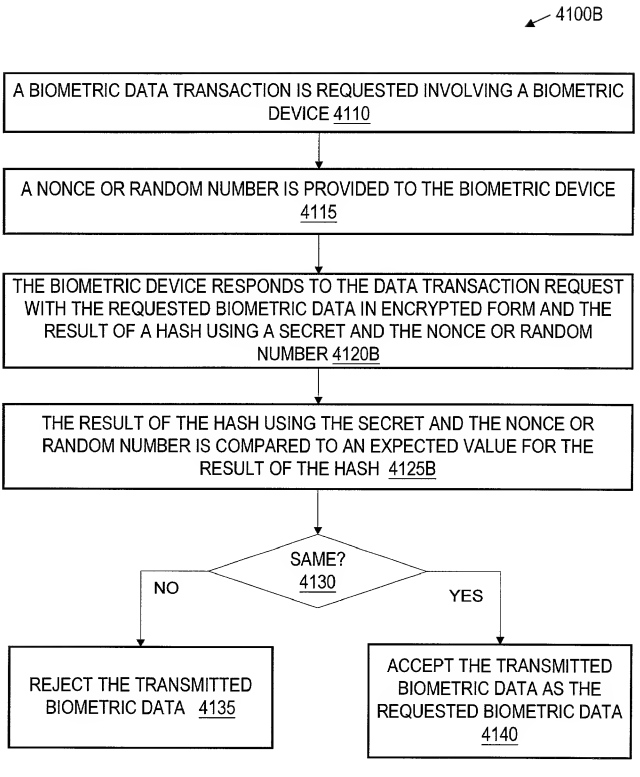

Fig. 30B

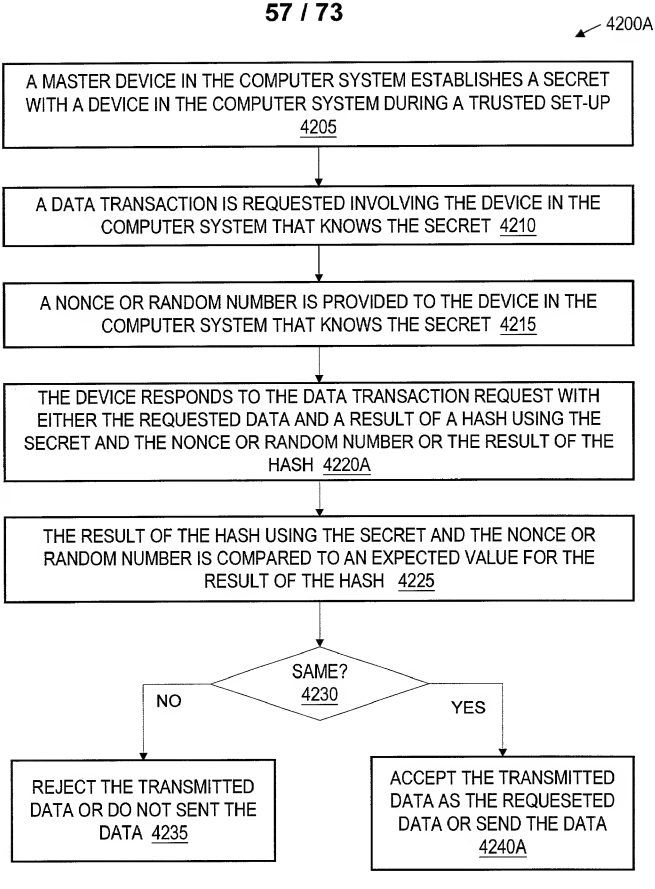

Fig. 31A

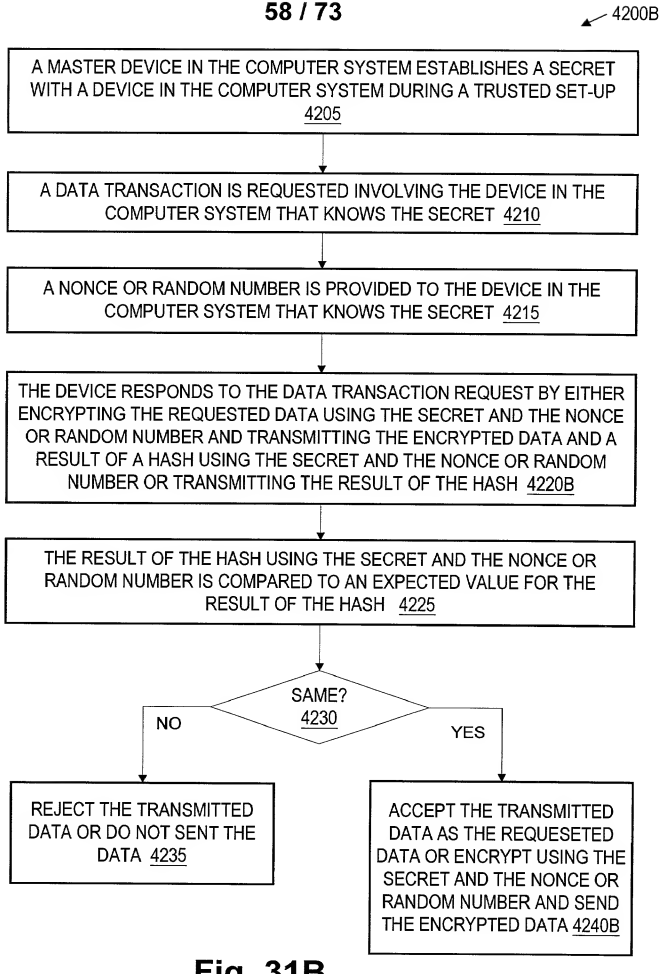

Fig. 31B

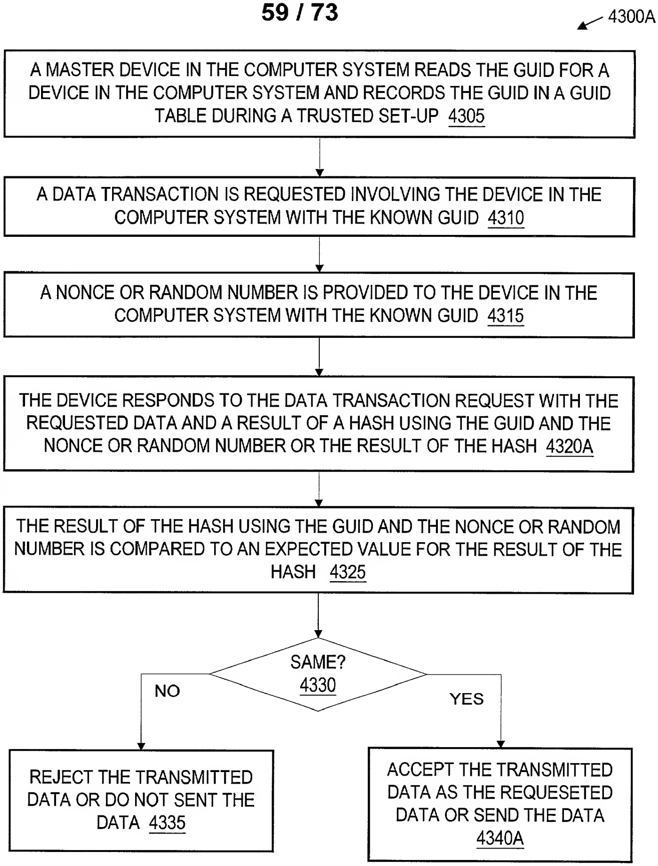
4300A
A MASTER DEVICE IN THE COMPUTER SYSTEM READS THE GUID FOR A DEVICE IN THE COMPUTER SYSTEM AND RECORDS THE GUID IN A GUID TABLE DURING A TRUSTED SET-UP 4305
A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID 4310
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID 4315
THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST WITH THE REQUESTED DATA AND A RESULT OF A HASH USING THE GUID AND THE NONCE OR RANDOM NUMBER OR THE RESULT OF THE HASH 4320A
THE RESULT OF THE HASH USING THE GUID AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4325
SAME? 4330
NO
YES
REJECT THE TRANSMITTED DATA OR DO NOT SENT THE DATA 4335
ACCEPT THE TRANSMITTED DATA AS THE REQUESETED DATA OR SEND THE DATA 4340A

Fig. 32A

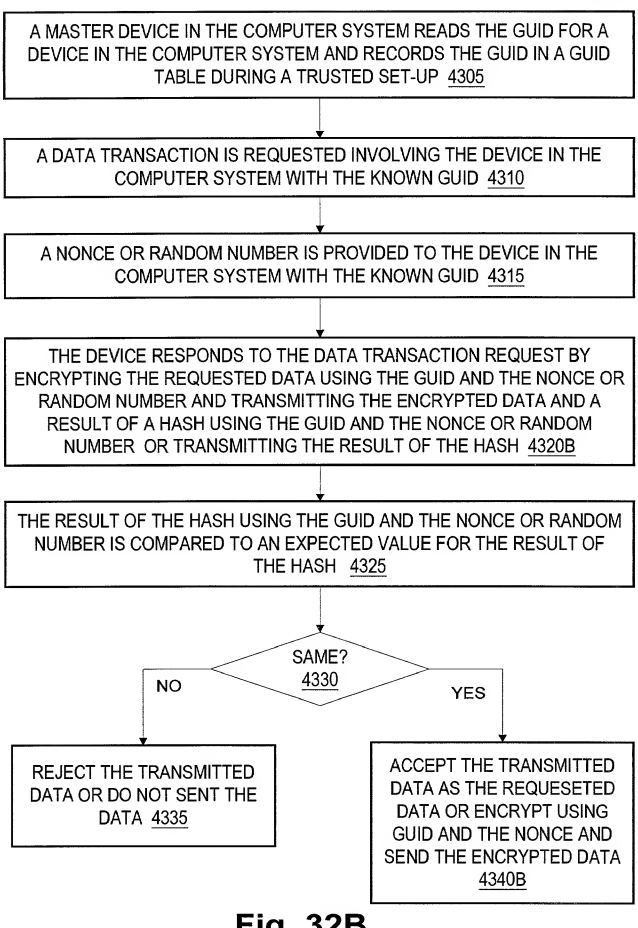

Fig. 32B

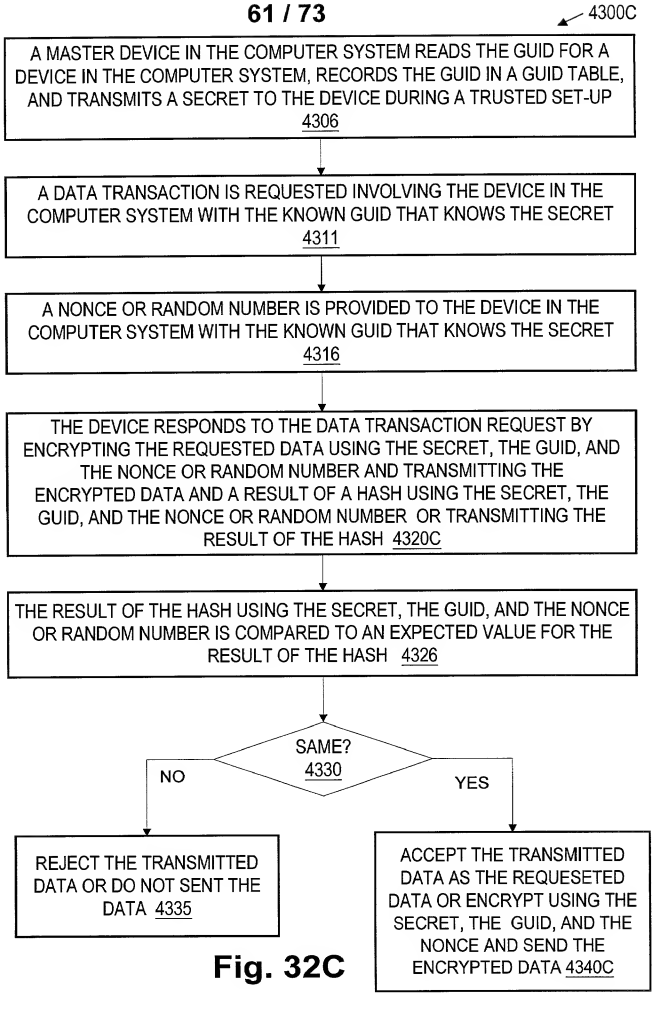

Fig. 32C

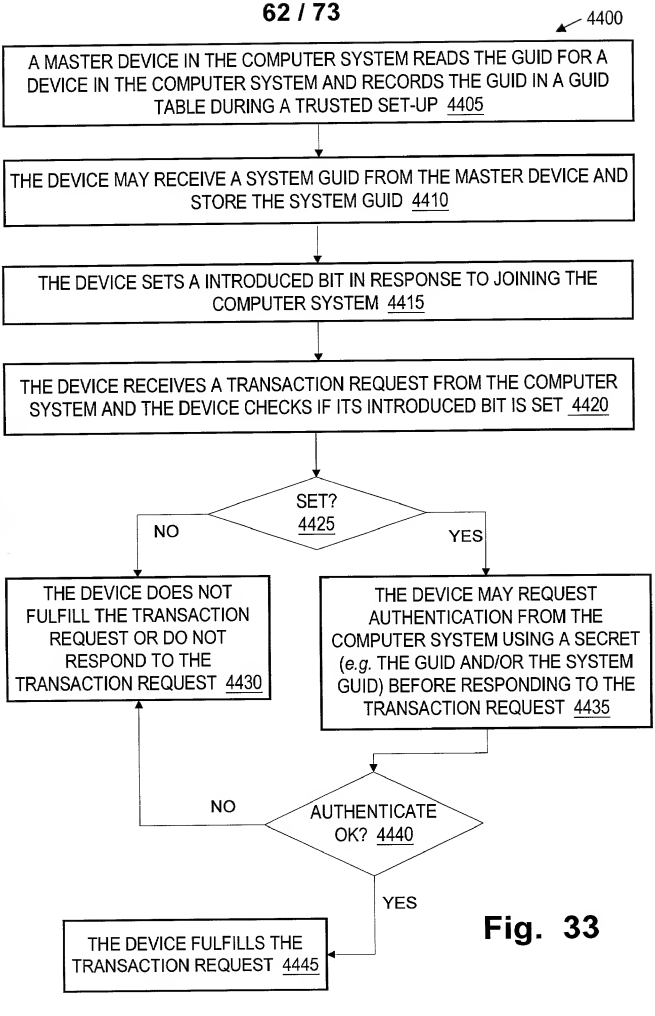

Fig. 33

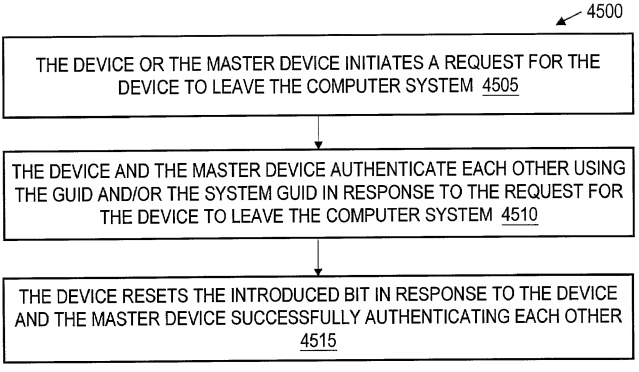

Fig. 34

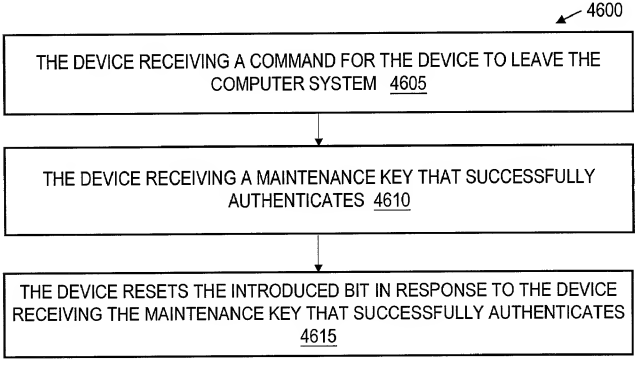

Fig. 35

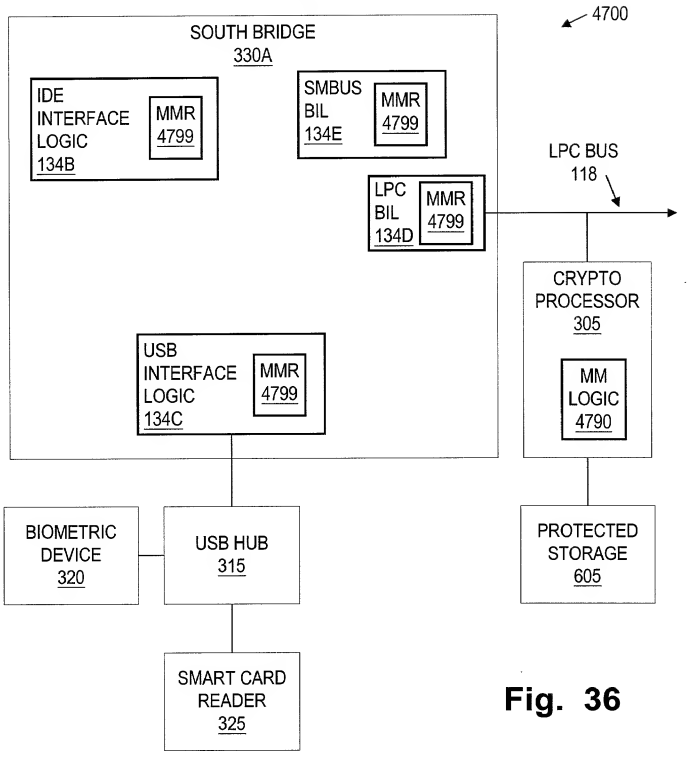

Fig. 36

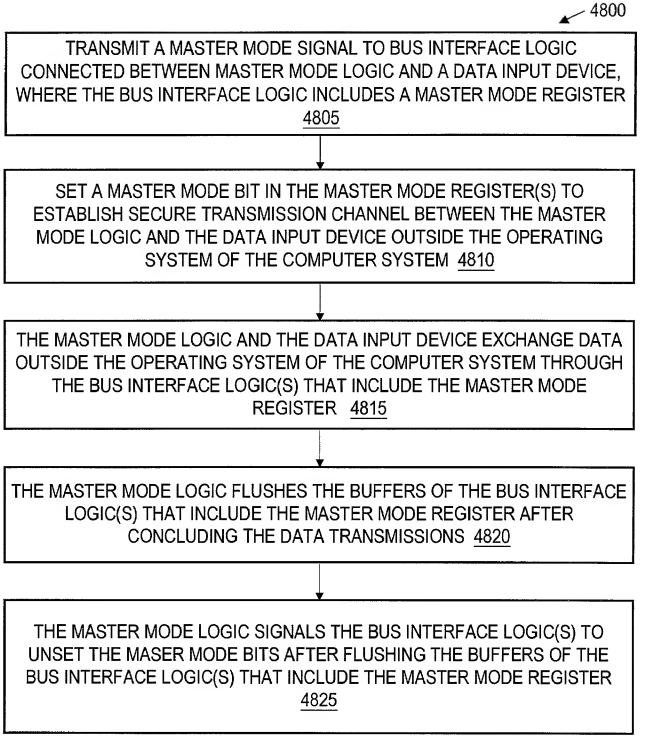

Fig. 37

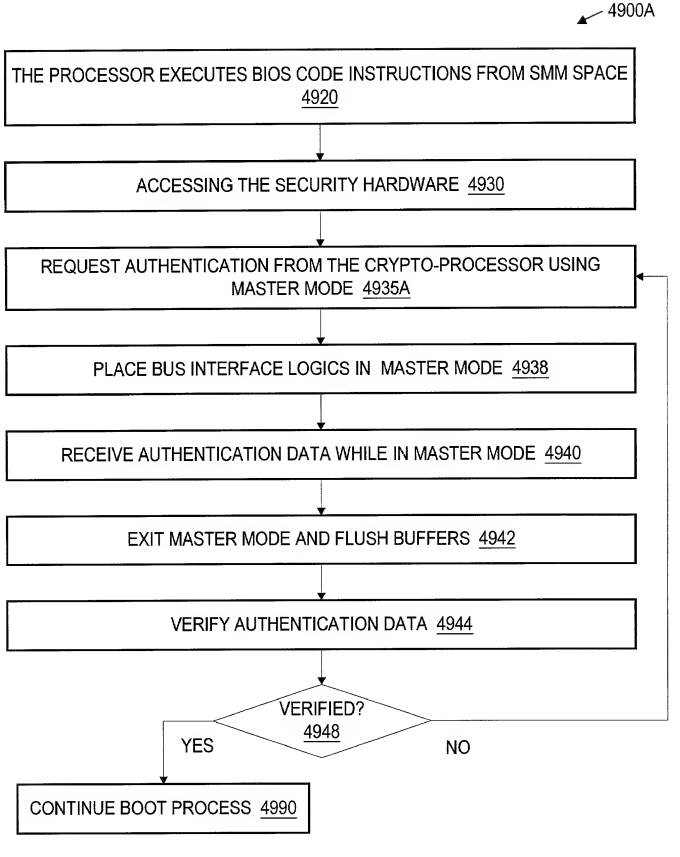
4900A
THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE 4920
ACCESSING THE SECURITY HARDWARE 4930
REQUEST AUTHENTICATION FROM THE CRYPTO-PROCESSOR USING MASTER MODE 4935A
PLACE BUS INTERFACE LOGICS IN MASTER MODE 4938
RECEIVE AUTHENTICATION DATA WHILE IN MASTER MODE 4940
EXIT MASTER MODE AND FLUSH BUFFERS 4942
VERIFY AUTHENTICATION DATA 4944
VERIFIED? 4948
YES
NO
CONTINUE BOOT PROCESS 4990

Fig. 38A

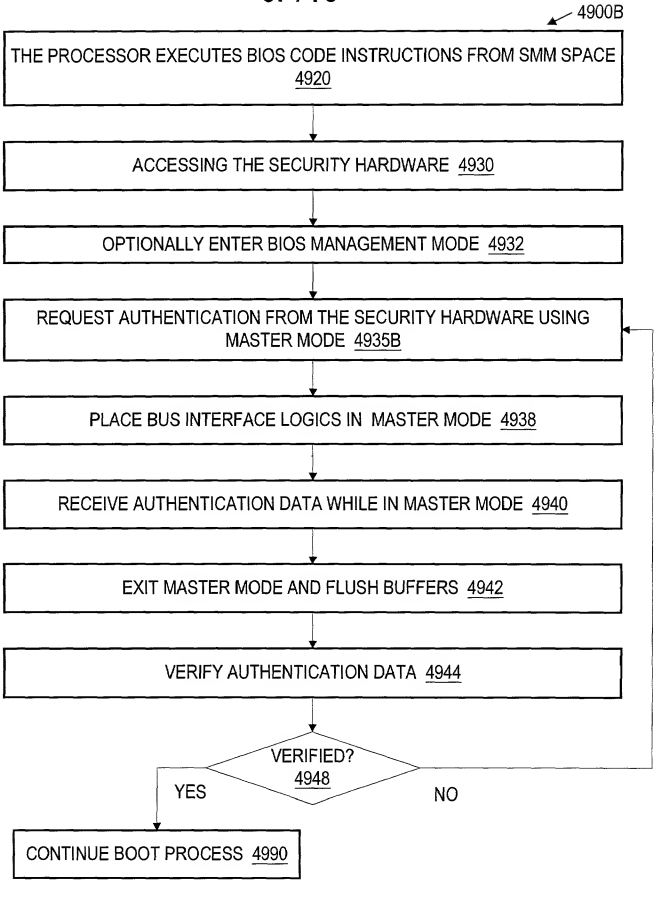
4900B
THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE 4920
ACCESSING THE SECURITY HARDWARE 4930
OPTIONALLY ENTER BIOS MANAGEMENT MODE 4932
REQUEST AUTHENTICATION FROM THE SECURITY HARDWARE USING MASTER MODE 4935B
PLACE BUS INTERFACE LOGICS IN MASTER MODE 4938
RECEIVE AUTHENTICATION DATA WHILE IN MASTER MODE 4940
EXIT MASTER MODE AND FLUSH BUFFERS 4942
VERIFY AUTHENTICATION DATA 4944
VERIFIED? 4948
YES
NO
CONTINUE BOOT PROCESS 4990

Fig. 38B

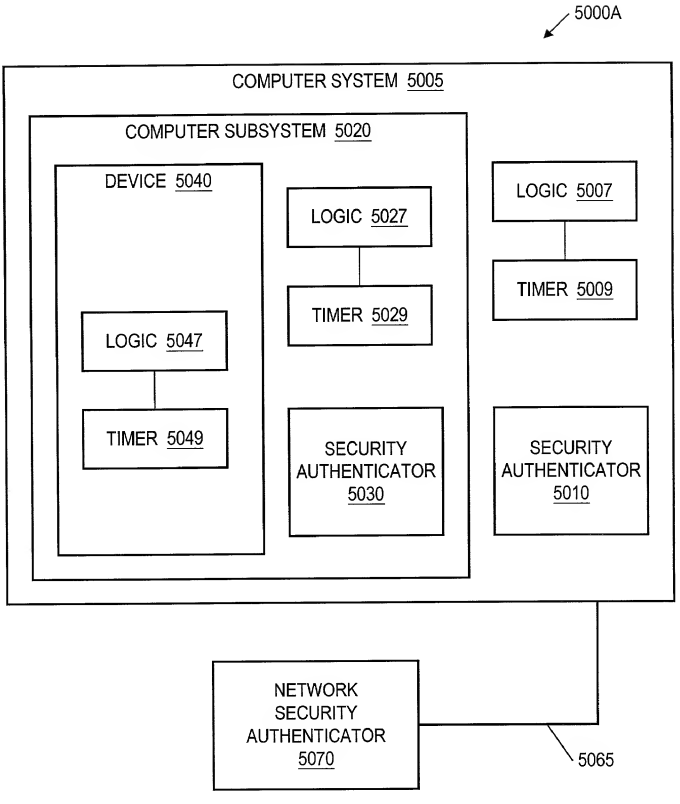

Fig. 39A

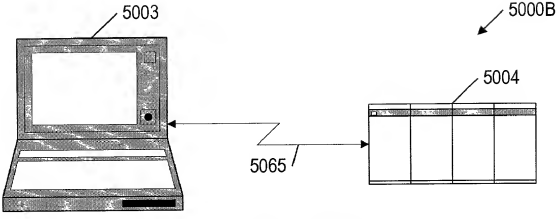

Fig. 39B

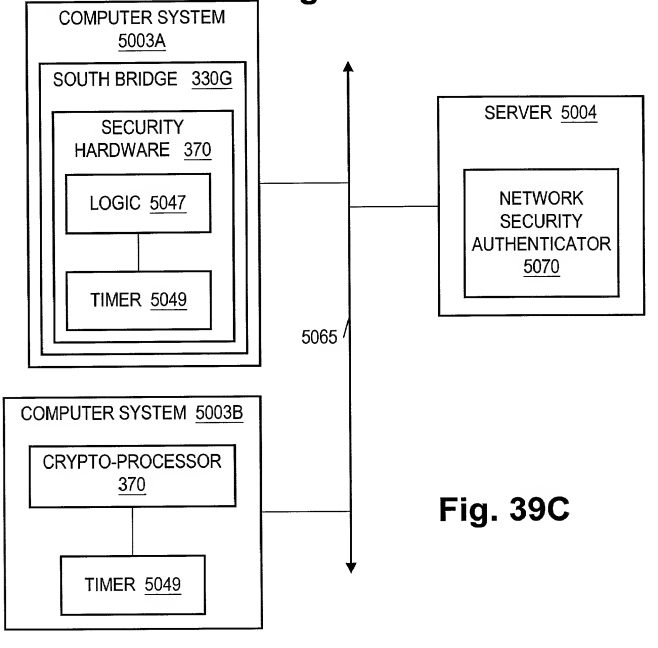

Fig. 39C

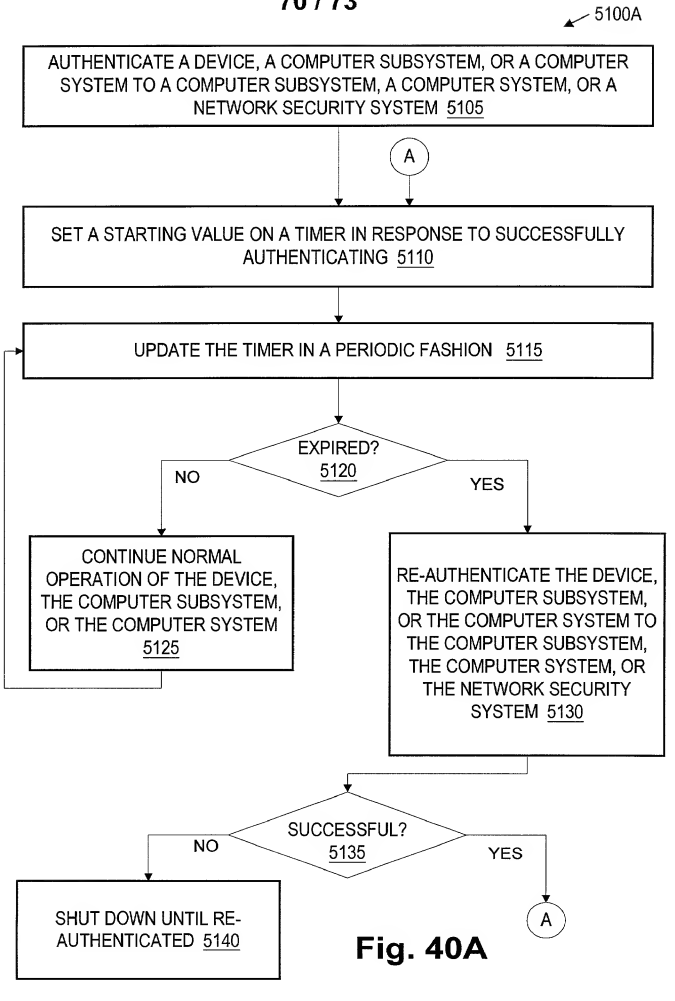

Fig. 40A

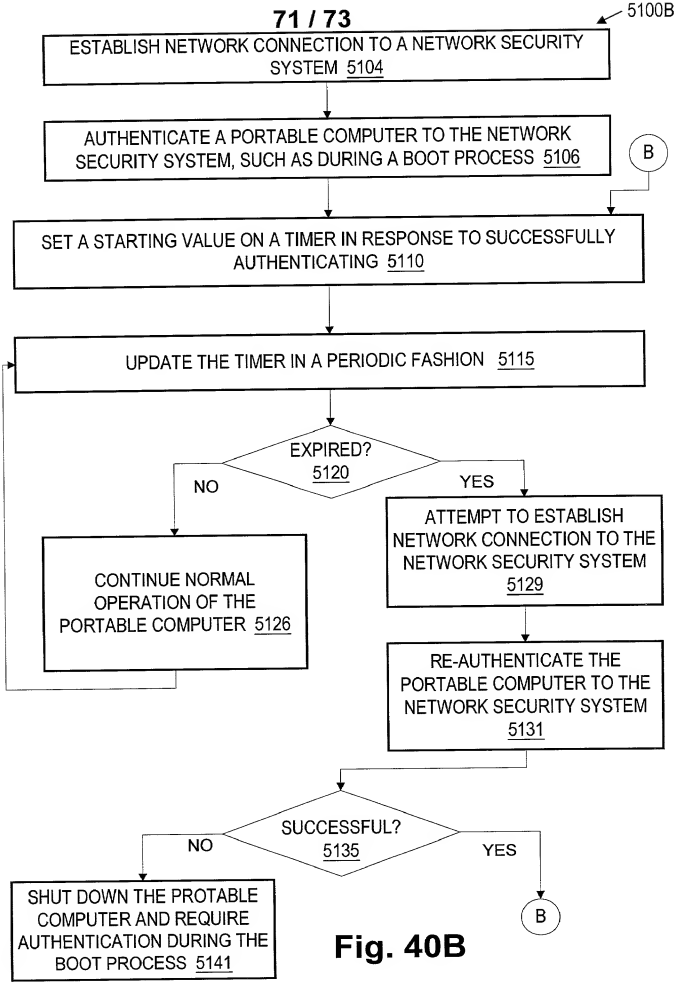

Fig. 40B

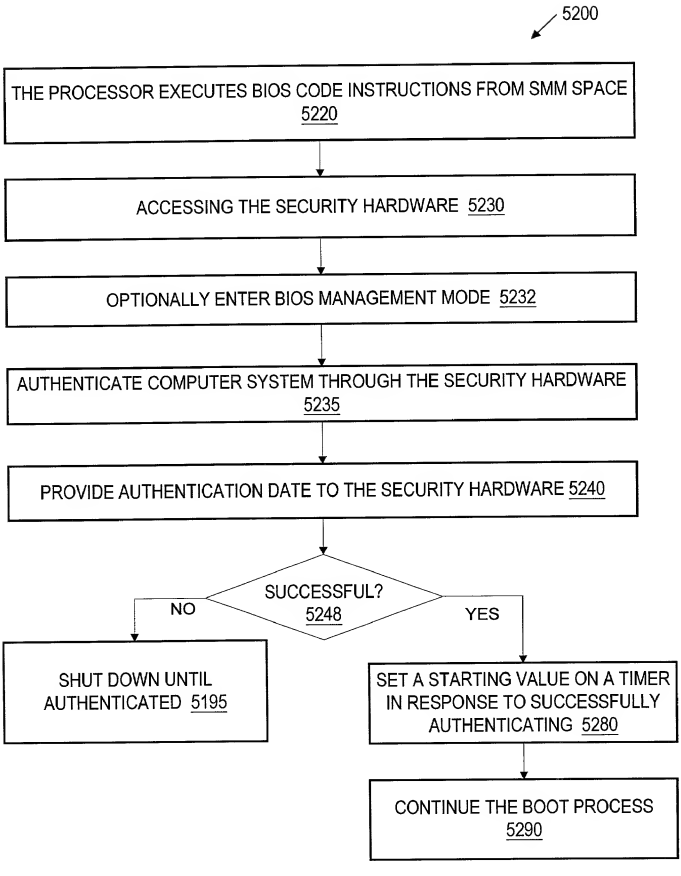

Fig. 41

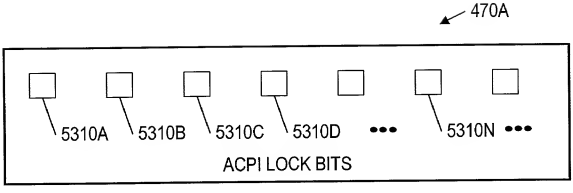

Fig. 42A

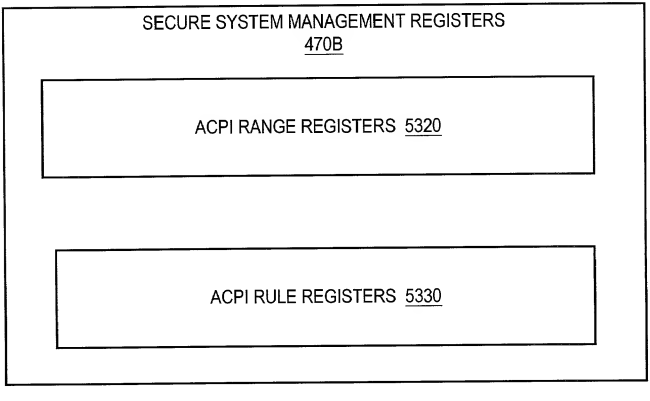

Fig. 42B